PATENT ABSTRACTS OF JAPAN

(11)Publication number: 10200530

(43)Date of publication of application: 31.07.1998

(51)Int.Cl.

H04L 12/24
H04L 12/26
G06F 13/00
H04L 12/46
H04L 12/28

(21)Application number: 09334093

(22)Date of filing: 04.12.1997

(71)Applicant: INTERNATL BUSINESS MACH CORP <IBM>

(72)Inventor: THEODORE JACK LONDON SCHRADER

(30)Priority

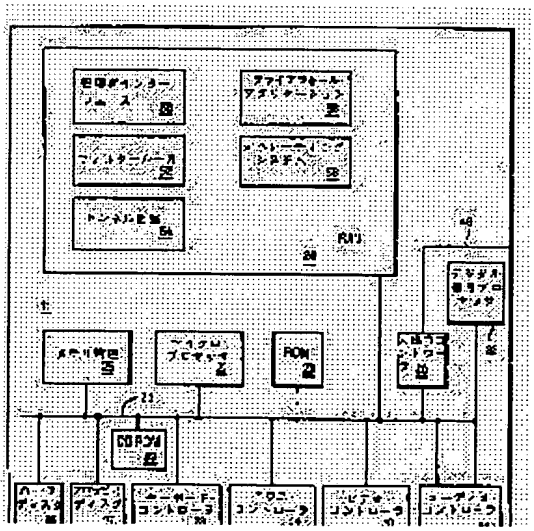
Priority number: 96 773542 Priority date: 23.12.1996 Priority country: US

(54) MANAGEMENT METHOD AND SYSTEM THEREFOR

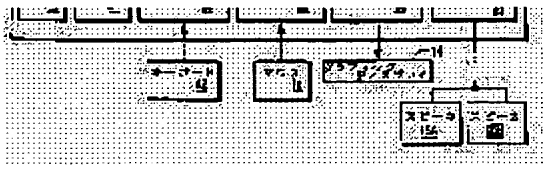
(57)Abstract:

PROBLEM TO BE SOLVED: To obtain a user-friendly interface for an internet protocol tunneling management of an internet fire wall by performing tunneling management of a fire wall computer between secure computer networks and computer networks that are not secure.

SOLUTION: A system unit 11 shows a graphic chart of tunnels among addresses of plural networks as lines that connect icons, which show network addresses on a display 14. The definition of a selection tunnel that is shown by a 1st line, according to the selection of a user of the 1st line, is shown in another partition of an interface. At this time, the



action to selection tunnel definition is available according to the input of the user. A graphic chart of tunnels is selectively changed by the user's input, and all the defined tunnels, etc., can be shown.



LEGAL STATUS

[Date of request for examination]	16.10.1998
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－200530

(43)公開日　平成10年(1998)７月31日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	12/24		Ｈ０４Ｌ	11/08	
	12/26		Ｇ０６Ｆ	13/00	３５５
Ｇ０６Ｆ	13/00	３５５	Ｈ０４Ｌ	11/00	３１０Ｃ
Ｈ０４Ｌ	12/46				
	12/28				

審査請求　未請求　請求項の数22　ＯＬ　（全 35 頁）

(21)出願番号　特願平9－334093

(22)出願日　平成９年(1997)12月４日

(31)優先権主張番号　０８／７７３５４２

(32)優先日　1996年12月23日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　セオドア・ジャック・ロンドン・シュレイダー
アメリカ合衆国78613、テキサス州、セダー・パーク、シャディー・ブルック・レイン　1704

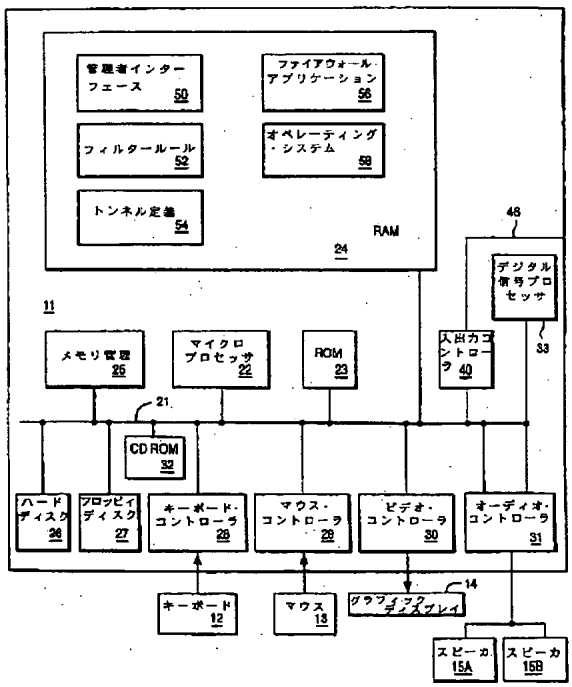
(74)代理人　弁理士　坂口　博　（外１名）

(54)【発明の名称】　管理方法およびシステム

(57)【要約】

【課題】　ウェブ・ベースのインターフェースで安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングの管理を提供すること。

【解決手段】　複数のネットワークのアドレス間のトンネルのグラフィック図がネットワーク・アドレスを示すアイコンを接続するラインとして表示される。第一ラインのユーザの選択に応じて、第一ラインによって示された選択トンネルの定義がインターフェースの別の区画（ペイン）に表示される。この時点で、選択トンネル定義へのアクションはユーザ入力に応じて行うことが可能である。トンネルのグラフィック図はユーザの入力により選択的に切り換えられ、全ての定義されたトンネルや、活動中のトンネルや、活動してないトンネル等を示すことができる。照会が入力トンネル定義について実行されて、既存のトンネル定義が入力トンネル定義と照合するかどうか判定する。



【特許請求の範囲】

【請求項１】安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータにおけるトンネリングを管理する方法において、複数のネットワークのアドレス間のトンネルのグラフィック図をネットワーク・アドレスを示すアイコンを接続するラインとして表示するステップと、
第一ラインのユーザの選択に応じて、その第一ラインによって示された選択したトンネル定義を表示するステップと、ユーザ入力に応じて、上記選択したトンネル定義へのアクションを行うステップとを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理する方法。

【請求項２】上記トンネルのグラフィック図は、ユーザ入力により、全ての定義したトンネルを示し、活動中のトンネルを示し、あるいは非活動中のトンネルを示すように選択的に変えることが可能であることを特徴とする、請求項１に記載の方法。

【請求項３】上記ラインは、各々のトンネルの特性を示す異なった方法で描かれていることを特徴とする、請求項１に記載の方法。

【請求項４】上記特性はトンネルに可能な安全状態であることを特徴とする、請求項３に記載の方法。

【請求項５】上記グラフィック図は各トンネルが発生してくる方向を示す印を有することを特徴とする、請求項１に記載の方法。

【請求項６】安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のコンピュータのトンネリングを管理する方法において、
トンネル定義を入れることのできる第一区画を有するユーザ・インターフェースを示すステップと、
ユーザ入力に応じて、入力されたトンネル定義と既存のトンネル定義が照合するか判定するために、入力されたトンネル定義についての照会を実行するステップと、
上記照会の結果を分散バーでユーザ・インターフェースの別な区画に表示し、トンネル定義の照合の位置は分散バーを通るラインにより示されるステップと、
ユーザ入力に応じて、選択トンネル定義についてのアクションを行うステップとを有することを特徴とするコンピュータのトンネリングを管理する方法。

【請求項７】第三区画でトンネル定義のリストを表示し、そこでは照合するトンネル定義が照合しないトンネル定義とは異なった方法で表示するステップと、
上記分散バーに隣接し、上記分散バーによって示されたトンネル定義の完全なリストに関して第三区画に表示したトンネル定義のリストの位置を示す小さなバーを表示するステップとを、さらに有することを特徴とする請求項６に記載の方法。

【請求項８】上記分散バーに隣接し、照合するトンネル定義の集中を示す小さなバーを表示するステップを、さらに有することを特徴とする請求項６に記載の方法。

【請求項９】安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理する方法において、
複数のネットワークのアドレス間のトンネルのグラフィック図をネットワーク・アドレスを示すアイコンを接続するラインとして表示するステップと、
第一ラインのユーザの選択に応じて、その第一ラインによって示された選択したトンネルに応用できるフィルタ・ルールのリストを表示するステップと、
ユーザ入力に応じて、上記選択したフィルタ・ルールへのアクションを行うステップとを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理する方法。

【請求項１０】ユーザ入力に応じて、選択したトンネルに既存のフィルタ・ルールが応用可能か判定するために、選択したトンネルについての照会を実行するステップと、
上記照会の結果を分散バーでユーザ・インターフェースの別な区画に表示し、フィルタ・ルールの照合の位置は分散バーを通るラインにより示されるステップとを更に有することを特徴とする、請求項９に記載の方法。

【請求項１１】照合するフィルタ・ルールを、フィルタ・ルールのリストの照合しないフィルタ・ルールとは異なった方法で表示するステップと、
上記分散バーに隣接し、上記分散バーによって示されたフィルタ・ルールの完全なリストに関して第三区画に表示したフィルタ・ルールのリストの位置を示す小さなバーを表示するステップとを、さらに有することを特徴とする請求項１０に記載の方法。

【請求項１２】安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理するためのプロセッサとメモリを有するシステムにおいて、
複数のネットワークのアドレス間のトンネルのグラフィック図をネットワーク・アドレスを示すアイコンを接続するラインとして表示する手段と、
第一ラインのユーザの選択に応じて、その第一ラインによって示された選択したトンネル定義を表示する手段と、
ユーザ入力に応じて、上記選択したトンネル定義へのアクションを行う手段とを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理するシステム。

【請求項１３】上記トンネルのグラフィック図は、ユーザ入力により、全ての定義したトンネルを示し、活動中のトンネルを示し、あるいは非活動中のトンネルを示すように選択的に変えることが可能であることを特徴とする、請求項１２に記載のシステム。

【請求項１４】上記ラインは、各々のトンネルの特性を示す異なった方法で描かれていることを特徴とする、請求項１２に記載のシステム。
【請求項１５】上記特性はトンネルに可能な安全状態であることを特徴とする、請求項１４に記載のシステム。
【請求項１６】上記グラフィック図は各トンネルが発生してくる方向を示す印を有することを特徴とする、請求項１２に記載のシステム。
【請求項１７】安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理するためのプロセッサとメモリを有するシステムにおいて、
トンネル定義を入力することのできる第一区画を有するユーザ・インターフェースを示す手段と、
ユーザ入力に応じて、入力されたトンネル定義と既存のトンネル定義が照合するか判定するために、入力されたトンネル定義についての照会を実行する手段と、
上記照会の結果を分散バーでユーザ・インターフェースの別な区画に表示し、トンネル定義の照合の位置は分散バーを通るラインにより示される手段と、
ユーザ入力に応じて、選択トンネル定義についてのアクションを行う手段とを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理するシステム。
【請求項１８】第三区画でトンネル定義のリストを表示し、そこでは照合するトンネル定義が照合しないトンネル定義とは異なった方法で表示する手段と、
上記分散バーに隣接し、上記分散バーによって示されたトンネル定義の完全なリストに関して第三区画に表示したトンネル定義のリストの位置を示す小さなバーを表示する手段とを、さらに有することを特徴とする請求項１７に記載のシステム。
【請求項１９】上記分散バーに隣接し、照合するトンネル定義の集中を示す小さなバーを表示する手段を、さらに有することを特徴とする請求項１７に記載のシステム。
【請求項２０】安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理するプロセッサとメモリを有するシステムにおいて、
複数のネットワークのアドレス間のトンネルのグラフィック図をネットワーク・アドレスを示すアイコンを接続するラインとして表示する手段と、
第一ラインのユーザの選択に応じて、その第一ラインによって示された選択したトンネルに応用できるフィルタ・ルールのリストを表示する手段と、
ユーザ入力に応じて、上記選択したフィルタ・ルールへのアクションを行う手段とを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理するシステム。
【請求項２１】ユーザ入力に応じて、選択したトンネルに既存のフィルタ・ルールが応用可能か判定するために、選択したトンネルについての照会を実行する手段と、
上記照会の結果を分散バーでユーザ・インターフェースの別な区画に表示し、フィルタ・ルールの照合の位置は分散バーを通るラインにより示される手段とを更に有することを特徴とする、請求項２０に記載の方法。
【請求項２２】照合するフィルタ・ルールを、フィルタ・ルールのリストの照合しないフィルタ・ルールとは異なった方法で表示する手段と、
上記分散バーに隣接し、上記分散バーによって示されたフィルタ・ルールの完全なリストに関して第三区画に表示したフィルタ・ルールのリストの位置を示す小さなバーを表示する手段とを、さらに有することを特徴とする請求項２１に記載の方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は分散型コンピュータ・ネットワークの安全システムに関する。特に、安全でないインターネットと安全な企業内ネット間に見られるようなコンピュータのＩＰトンネリングを管理するためのウェブ・ベースのインターフェースに関する。
【０００２】本出願は、共通の譲渡人による米国特許出願である１９９６年１２月２３日出願、出願番号７７３５４３、発明者Ｔ．Ｓｈｒａｄｅｒによる「インターネット・ファイアウォールのＩＰフィルタ処理のウェブ・ベースの管理」に関連した発明である。
【０００３】
【従来の技術】インターネット管理者の負担は急速に量や複雑さが増大してきた。企業あるいは組織の安全な内部ネットを外部の安全ではないインターネットに接続するインターネット・ファイアウォールを管理するために複数の管理者と協力する、管理責任者が必要である。従来技術では一般に、ファイアウォールのインターフェースは管理者がインターネット・ファイアウォール特性とオペレーションを管理する事を可能にするコマンド・ラインあるいはＳＭＩＴインターフェースである。これらのタイプのインターフェースは多くのコマンドの記憶化を要求し、また、管理者はファイアウォールを支配するトンネル・ルールを管理するために異なったアクションからの出力を継ぎ合わせる必要がある。これは管理者が複数のスクリーンからの情報を記憶したり、ライトダウンしなければならない時に、明らかに不便である。つまり、従来のインターフェースは決してユーザにとって扱い易いわけではない。
【０００４】
【発明が解決しようとする課題】本発明はインターネット・ファイウォールのＩＰトンネリングの管理のためにユーザが使い易いインターフェースを提供することを目

的とする。

【０００５】さらに、本発明の目的はファイアウォール・コンピュータのＩＰトンネリングを管理するためのインターフェースを改良することである。

【０００６】

【課題を解決するための手段】上記目的は、安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理することにより達成される。

【０００７】望ましい一実施例では、複数のネットワークのアドレス間のトンネルのグラフィック図がネットワーク・アドレスを示すアイコンを接続するラインとして表示される。第一ラインのユーザの選択に応じて、第一ラインによって示された選択トンネルの定義がインターフェースの別の区画（ペイン）に表示される。この時点で、選択トンネル定義へのアクションはユーザ入力に応じて行うことが可能である。トンネルのグラフィック図はユーザの入力により選択的に切り換えられ、全ての定義されたトンネルや、活動中のトンネルや、活動してないトンネル等を示すことができる。

【０００８】本発明の別の実施例では、ユーザ・インターフェースは一つのトンネル定義を入れることのできる第一区画を持つように提供される。照会が入力トンネル定義について実行されて、既存のトンネル定義が入力トンネル定義と照合するかどうか判定する。この照会の結果がユーザ・インターフェースの別の区画に分散バーで表示され、照合したトンネル定義の位置をその分散バーを通ったラインにより示される。小さなバーが分散バーの近くで表示され、その小さなバーは分散バーにより示されたトンネル定義の全リストに関係のあるトンネル定義の表示リストの位置を示している。この時点で、一つの選択したトンネル定義についてアクションが行える。

【０００９】本発明のさらに別な実施例では、ネットワークにおけるアドレス間のトンネルのグラフィック図が、ネットワーク・アドレスを示すアイコンに接続するラインとして提供される。第一ラインのユーザの選択に応じ、第一ラインにより示された選択トンネルに適用可能なフィルタ・ルールのリストが表示される。分散バーはユーザ・インターフェースの別の区画に表示される。そこで、分散バーにより示される全てのフィルタ・ルールのリスト内で、フィルタ・ルールと照合する位置が分散バーを通るラインにより示される。この時点で、ユーザ入力に応じ、選択したフィルタ・ルールについてアクションを行うことができる。

【００１０】

【発明の実施の形態】本発明は複数の異なったオペレーティング・システム下にある種々のコンピュータあるいは複数のコンピュータの集まりで実行できる。例えば、コンピュータはパーソナル・コンピュータ、ミニ・コンピュータ、メインフレーム・コンピュータ、あるいは他のコンピュータの分散ネットワークで実行するコンピュータ等である。コンピュータの選択はプロセッサ速度やディスク記憶の要求などによってのみ制限されるが、ＩＢＭ ＰＣシリーズのコンピュータは本発明に使用可能である。ＩＢＭパーソナル・コンピュータが実行できるオペレーティング・システムの一つはＩＢＭのＯＳ／２ Ｗａｒｐ４．０である。別に、コンピュータ・システムがＡＩＸ（登録商標）オペレーティング・システムで実行するコンピュータのＩＢＭ ＲＩＳＣシステム／６０００（登録商標）ラインにある。

【００１１】図１では、システム・ユニット１１、キーボード１２、マウス１３、ディスプレイ１４を有するコンピュータがブロック図で示されている。システム・ユニット１１は、種々の構成部品が接続されている単独のシステム・バス、あるいは複数のシステム・バス２１を有し、それにより種々の構成部品間で通信が行われる。マイクロプロセッサ２２はシステム・バス２１に接続され、またシステム・バス２１に接続されている読取り専用メモリ（ＲＯＭ）２３とランダム・アクセス・メモリ（ＲＡＭ）２４によりサポートされている。ＩＢＭ ＰＣシリーズのコンピュータのマイクロプロセッサはIntel386、486あるいはPentiumマイクロプロセッサ等の一種である。しかし、Motorola社の68000、68020、68030等のマイクロプロセッサも、特に限定されないが使用でき、またＩＢＭ社のPower PCチップのような縮小命令セット・コンピュータ（ＲＩＳＣ）も含まれる。Hewlett Packard、 Sun、 Motorola社等により作られた他のＲＩＳＣチップもこのコンピュータに使用可能である。

【００１２】ＲＯＭ２３は、特に、対話およびディスク・ドライブ、キーボードのような基本的なハードウェア・オペレーションを制御するＢＩＯＳ（基本動作命令プログラム群）を含む。ＲＡＭ２４は、オペレーティング・システムやアプリケーション・プログラムをロードされている主メモリである。メモリ管理チップ２５はシステム・バス２１に接続されており、ＲＡＭ２４とハード・ディスク・ドライブ２６およびフロッピイ・ディスク・ドライブ２７間のデータを含み、通過させる直接メモリ・アクセス・オペレーションを制御する。システム・バス２１に接続したＣＤ-ＲＯＭ３２も、例えばマルチメディア・プログラムや図形表示のような多量のデータを記憶するために使われる。

【００１３】また、このシステム・バス２１に種々の入力／出力コントローラを接続しており、例えばキーボード・コントローラ２８、マウス・コントローラ２９、ビデオ・コントローラ３０、オーディオ・コントローラ３１などである。既知のごとく、キーボード・コントローラ２８はキーボード１２のハードウェア・インターフェースを提供し、マウス・コントローラ２９はマウス１３のハードウェア・インターフェースを提供し、ビデオ・コントローラ３０はディスプレイ１４のハードウェア・

インターフェースであり、オーディオ・コントローラ３１はスピーカ１５のハードウェア・インターフェースである。トークン・リング・アダプタのような入力／出力コントローラ４０は、ネットワーク４６を通じて、同様に構成された他のデータ処理システムとの通信を可能とする。

【００１４】本発明の望ましい実行例の一つは、上記したように構成した１つ以上のコンピュータ・システムのＲＡＭ２４にある複数の命令５０－５８のセットである。コンピュータ・システムが要求するまで、その命令セットは、例えば、ハード・ディスク・ドライブ２６、あるいは取り出し可能なメモリ、つまりＣＤ-ＲＯＭ３２で随時使用できる光ディスクや、フロッピイ・ディスク・ドライブ２７で随時使用できるフロッピイ・ディスク等の、別のコンピュータで読取り可能なメモリに記憶させることができる。さらに、その命令セットは別のコンピュータのメモリに記憶させることが可能であり、またユーザの望みによりローカル・エリア・ネットワークやインターネットのようなワイド・エリア・ネットワークを通じて送信することができる。この命令セットの物理的な記憶は電気的、磁気的、あるいは化学的に記憶させた媒体を物理的に変更し、その媒体はコンピュータが読取り可能な情報を担持することは当業界では公知である。本発明を命令、記号、文字等について説明することは便利であるが、それらの全ておよび同様な用語は適切な有形の構成要素と関連させるべきである。

【００１５】さらに、本発明は頻繁に比較あるいは確認すること、または人間のオペレータと組み合わせることが可能な表現で説明する。人間のオペレータによるアクションを行わないことが、本発明の一部を形成するオペレーションで望ましい。このオペレーションは他の電気信号を発生する電気信号を処理する機械操作である。

【００１６】ＩＢＭ社のSecure Way Firewall（ＳＷＦ）のようなインターネットのファイアウォール製品は、インターネットの内部安全ネットワークと外部の安全でないネットワーク間の物理的なファイアウォールを管理者が作ることを可能とする。ファイアウォール装置の物理的な接続のほかにも、ファイアウォール製品は、安全なネットワークから出し入れする情報の流れを管理者が制御することを助ける複数の機能を提供する。そうした機能はテルネット（telnet）、ＦＴＰ代理サービス、ＳＯＣＫＳサービス、特別のドメイン名サービス、安全なネットワーク間のインターネット中のＩＰトンネリング、ＩＰパケットの安全ネットワークへの出入りを許可、あるいは拒絶の判定をするためのフィルタ・ルールの実行等である。

【００１７】こうしたフィルタ・ルールの一つはＩＰの偽物に対する防護を行うことであり、そのＩＰの偽物とは、アタッカがあるＩＰパケットを変えて、そのアタッカのワークステーションと同じではないソースＩＰアドレスから来たかのように見せようとすることである。管理者はＩＰフィルタを設定し、安全なネットワークに対し内部にあるが、安全ではないネットワークから来ているソースＩＰアドレスを有するＩＰパケットを拒絶する。

【００１８】図２は２つのネットワークを利用するファイアウォール構成の一例を示す。ここでは、一つの装置１００だけが防護拠点としてファイアウォールに含まれており、すべてのＩＰパケットはこの装置を介して安全でないネットワーク１１０から安全なネットワーク１２０へ、あるいはその逆へ送られる。このファイアウォール装置１００は、ファイアウォールで実施可能あるいは実施不可能なアプリケーション・ゲートウェイに対するファイアウォールの置き換えに加えて設けられたスクリーニング・フィルタ、またはＩＰフィルタを有している。

【００１９】図３はスクリーニング・フィルタを有する別の装置１４０の後ろに防護装置１３０を配置した、別の構成を示している。この構成は、ＩＰパケットが防護装置のアプリケーション・ゲートウェイによって処理される前に、初めにファイアウォールを通って許可されなければならないので、さらにファイアウォールに対する防護を提供することになる。安全でないネットワークおよび安全なネットワークが、それぞれ１５０１６０に示されている。

【００２０】ＩＰトンネリングは、本発明の主題であるインターネット・ファイアウォールにより提供された機能である。管理者は、ＩＰパケットが流れる２つのインターネット防護壁間のトンネルを定義することができる。管理者がＩＰトンネルをどのように定義したかに応じてファイアウォール間のインターネットを流れるＩＰパケットを符号化するのと同時に、このトンネルはソースと宛先アドレス間に立証を課す。

【００２１】ＩＰトンネルの全体的な説明は、バーチャル・プライベート・ネットワーク（ＶＰＮ）のインターネット技術者のタスク・フォース（ＩＥＴＦ）で与えられる。

【００２２】ファイアウォールによって行うＩＰトンネリングやフィルタ処理のプロセスは公知技術では詳細な説明はされていない。さらに、それらはハードウェアに影響されるだけでなく、特別なファイアウォール技術により変化する。以下に説明するウェブ・ベースのインターフェースは、ユーザ入力に応じた必要な機能を行うためにＡＰＩあるいは他のソフトウェア・インターフェースを介してファイアウォールを単に呼び出すだけである。これは実用的ではないが、ファイアウォールの機能はインターフェースを有するウェブ・ページに複製される。

【００２３】ファイアウォール・コンピュータそのものに残らなくてはならない公知技術のインターフェースと

は逆に、本発明のウェブ・ベースのインターフェースは管理者のシステムとファイアウォール・システム間で求められる適切な安全性を有するネットワークのどのコンピュータにも残ることができる。インターフェースは安全なネットワーク内のファイアウォールあるいは別のシステムにあることが可能であるが、ファイアウォールの管理も特に信用のあるアドレスで安全なネットワークの外側で起こすことも可能である。しかし、これは安全の観点からあまり望ましいものではない。それにも拘わらず、このインターフェースは軽便であり、従来技術では不可能だった柔軟性を管理者に与えることができる。

【００２４】上記説明のように、従来技術のインターフェースは通常、管理者が不可解な多数のコマンドを学習することを強いられるコマンド・ラインを基本としている。本発明はウェブ・ベースのユーザ・インターフェースのフレームワークを用いる。ＩＰトンネルに対する管理者のタスクは、ＩＰトンネルの定義、ＩＰトンネルのグラフィック表示、ＩＰトンネルの照会、ＩＰトンネルの定義を有するＩＰフィルタ・ルールの照会等に分けられる。望ましい一実施例では、ユーザ・インターフェースは次のウェブ・ページに分けられる。

【００２５】＊ＩＰトンネルの定義のページ
＊ＩＰトンネルのグラフィックスのページ
＊ＩＰトンネルの照会のページ
＊ＩＰトンネル／フィルタの照会のページ

【００２６】これらのページの詳細な説明をする。すなわち、本発明は、ウェブ・ベースの管理ブラウザの全ての機能のセットを管理者がインストール、あるいは使用する必要がないような設計モジュールである。管理者がフィルタ・ルールの管理にだけ関心があるなら、ＳＯＣＫＳサーバやＩＰトンネリングに対してのような、その他の管理機能に繋がるパスは引用する必要がない。他の機能は必要な時にプラグ・インさせることが可能である。

【００２７】本発明は、従来技術のインターフェースでは有効ではなかったウェブ・ベースのファイアウォール・フレームワークへＩＰトンネリングに関する多くの機能を加え、同時にその低レベルのページの配置を矛盾無く維持する。このモジュール・レベルの各ページは複数の区画（あるいはフレーム）に分割され、各区画はページに関係なく特定のタイプの情報を表示する。従って、管理者は情報があるページに応じた情報の前後関係を予測することができる。

【００２８】典型的なページのレイアウトを以下に説明する。図４にはＩＰトンネル定義ページが示されている。ナビゲーション区画２００がこのページの最上部に示される。この区画により、管理者はテキストかアイコンを選択してファイアウォール・インターフェースの管理モジュールか他のモジュールの他の部分をナビゲートする。

【００２９】ナビゲーション区画２００の下には、ディスプレイ区画２１０とディスプレイ・アクション区画２２０が表示されている。ディスプレイ区画２１０はエントリ・フィールド２１２あるいはアクティブ・ファンクションの押しボタン２１４を示すページの場所を提供する。スクロール・バー２１６を別のエントリ・フィールド用に設ける。他の区画には、そのページの初めの情報のグラフィックス表示が示される。ＩＰトンネルのグラフィックス・ページに対して、この区画は安全なネットワーク間の接続を絵画的に示すことになる。

【００３０】ディスプレイ・アクション区画２２０は、管理者が押しボタン２２２によりディスプレイ区画のオブジェクトの定義を修正したり、保存することを開始可能なアクションを提供する。あるいは、管理者によって開始されたアクション（図示せず）の結果を示す。

【００３１】このページの次のレベルはメータ区画２３０、リスト区画２４０、リスト・アクション区画２５０に分割されている。このレベルの主区画はリスト区画２４０であり、これは管理者が該当区画に属する全てのエントリを見ることを可能とする。ＩＰトンネル定義のページについて、リスト区画が定義ずみのＩＰトンネルのリスト２４２を管理者に示す。スクロール・バー２４４、２４６は別のエントリや複数のエントリについての情報を表示するためのオプション的な機能である。

【００３２】リスト・アクション区画２５０は、ディスプレイ・アクション区画と同じように動作する。管理者は押しボタン２５２を作動させてリスト区画のエントリに関連するアクションのリストから、ＩＰフィルタ・ルールの完全なリストを記憶、あるいは目標最終点のファイアウォールにＩＰトンネル定義のリストを送ること等を選択できる。

【００３３】メータ区画２３０は、表示区画により開始させられた統計、あるいはリスト区画内の全統計に関する情報を画像的あるいは文章的表現で表示する。トンネル定義ページにおいて、トレースルート、ピーンという音、指によるルーチンの出力が表示される。

【００３４】チッカ・テープ区画２６０はこのページの一番下にあり、このページのエントリやオブジェクトについての動的情報や統計的情報を管理者に提供する。情報は右から左にスクロールし、管理者がこのページでアクションを開始する際に更新される。

【００３５】望ましい実施例では、ウェブ・ベースの管理ページは、Netscape Navigator（登録商標）ブラウザのような、htmlやJava（登録商標）アプレットを支援するウェブ・ブラウザにおいて使用できる。図から明らかなように、全てのウェブ・ページは管理者に対して矛盾のない使い易いレイアウトを提供する。

【００３６】ＩＰトンネル定義ページを詳細に説明する。ＩＰトンネル定義ページは管理者が次のアクションを行うことを可能にする。

＊　あるファイアウォールについて記憶したＩＰトンネル定義を見る。
＊　新しいＩＰトンネル定義を作る。
＊　記憶したＩＰトンネル定義を修正する。
＊　ＩＰトンネル定義をロードあるいは保存する。
＊　記憶したＩＰトンネル定義を配布する。
＊　記憶したＩＰトンネル定義を活性化あるいは不活性化する。
＊　ＩＰトンネル定義を停止する。
＊　２つのファイアウォール間でＩＰトンネル定義を確認する。

【００３７】管理者はディスプレイ区画２１０のエントリ・フィールド２１２やリスト・ボックス２１４、およびディスプレイ・アクション区画２２２の押しボタン２２２アクションを使ってＩＰトンネル定義を作成したり、修正したりできる。リスト区画２４０はインターネット・ファイアウォール用に定義された全てのＩＰトンネル定義を表示する。管理者はそれらをスクロールし、修正または削除用のＩＰトンネル定義を明るく点灯させ、リスト・アクション区画２５０の押しボタン２５２により一つのアクションを選択して、ファイアウォールに送る等のＩＰトンネル定義についてのオペレーションを行う。

【００３８】ウェブ管理ブラウザが実行されるホストの目標ＩＰアドレスに管理者がアクセス可能なら、その管理者はエントリ・フィールドに隣接した適切なボタンを押すことにより、目標ＩＰアドレスをピンと鳴らす、トレースルートする、指で指示することが可能である。例えば、管理者はソース・アドレスに隣接したピン・ボタンを押すと、インターフェースはソース・アドレス・フィールドのピン・プロセスを実行する。これらのアクションの出力はメータ区画２３０に現れる。および別の方法でテープ区画２６０をチッカ作動する。この機能は、管理者がインターフェースから離れる必要なくＩＰアドレスが到達可能、あるいは識別可能か容易に判定する。チッカ・テープ区画もＩＰトンネル定義についての統計的情報、つまり同じソースと宛先アドレス間で定義されたトンネルの数等の情報をピン機能あるいは指機能の出力を表示するために使われてない時に、表示する。

【００３９】ここでは、この図に示されているインターフェースから始めることができるシステム・アクションの全てが説明されている訳ではなく、このウェブ・ページで実行可能なアクションの説明である。

【００４０】図５のＩＰトンネル画像ページは、２つのインターネット・ファイアウォール間で定義されたＩＰトンネルを管理者が画像的に見ることを可能にする。このウェブ・ページは、左側のファイアウォールのソース・アドレスを表すボックス３１３と右側の目標ファイアウォールの宛先アドレスを表すボックス３１４、３１５、３１６を有するディスプレイ区画３１０に画像３１２を示している。ＩＰトンネルが２つのアドレス間で定義されている場所で、このウェブ・ページは２つのボックス間にライン３１７を引き、そのラインにシンボル３１８を付けてどのアドレスがそのトンネルを開始するか、およびそのＩＰトンネルのＩＤを示す。このラインは異なった種類を使用して引かれ、安全状態のような特性を示す。つまり、このトンネルが符号化あるいは認可可能であるか、あるいはその組合せが可能であるかどうか示す。ディスプレイ・アクション区画３２０は、管理者がボタン３２２、３２４、３２６を押すことにより、定義されたＩＰトンネル定義の全て、ファイアウォールで活動中のものだけ、あるいはファイアウォールで活動中ではないものだけを見ることを可能とする。

【００４１】メータ区画３３０はディスプレイ区画のＩＰトンネル・ラインの説明３３３を表示する。望ましい一実施例では、この区画は同様に他の動的情報も表示する。

【００４２】リスト区画は、このファイアウォールについて定義したＩＰトンネル定義の全てのスクロール可能なリスト３４２を表示することになる。管理者はこのディスプレイ区画３１０のＩＰトンネル・ラインを選択して点灯したウェブ・ページを有し、またリスト区画３４０内に全てのトンネル定義３４２を示す。リスト・アクション区画３５０の押しボタン３５２により管理者は、あるファイアウォールについての選択したＩＰトンネル定義を活性化したり、不活性化したり、編集したり、削除したりすることに加え、ＩＰトンネル定義のリストをロードあるいは保存することが可能である。

【００４３】この図に示されているアクションの全てが説明されている訳ではなく、このウェブ・ページで実行可能なアクションの説明である。

【００４４】図６はＩＰトンネル照会ページを示しており、記憶したＩＰトンネル定義集合に対して管理者が照会を実行してその照会と照合する全ての定義を見ることができる。照会も複数のワイルドカードをサポートする。例えば、ある宛先への照会で特定した基準と照合した、あるＩＰトンネル定義をリターンさせるワイルドカードで、宛先アドレスを特定することができる。

【００４５】管理者は照会ページのディスプレイ区画４１０で照会を定義することができる。トンネルＩＤのエントリ・フィールド、ソース・アドレス、宛先アドレス、符号化アルゴリズム、符号化ポリシィ等が設けられている。望ましい一実施例では、以前の照会は新たな照会のモデルとして、あるいは修正せずに再度実行させるために、保存、検索、表示等ができる。反復の実行が考えられる照会を保存することは利点が多い。このリストのＩＰトンネル値から誘導した選択リストは、ＩＰトンネルのリストのＩＤとアドレスのセットからＩＰトンネルＩＤまたはアドレスのリストを提供する。

【００４６】図に示したように、ディスプレイ・アクシ

ョン区画４２０は、ディスプレイ区画をクリアする押しボタン４２２とディスプレイ区画で定義した照会の実行４２４の２つのアクションを管理者に提供する。このディスプレイ・アクション区画４２０も、照会テストと照合したＩＰトンネル定義の数を示す大きな字体の数字４２６を表示する。

【００４７】メータ区画４３０は照合したＩＰトンネル定義の分布を視覚的に示すグラフィカル・バー４３２を表示する。これらの照合したＩＰトンネル定義はバーの他の部分とは異なる色を着けられている。このバー４３２は、視覚的かつ迅速に照合したＩＰトンネル定義およびＩＰトンネル定義リスト内の分布を示すので分散バーと呼ばれる。この分散バー４３２に隣接した小さなバー４３４が位置的なキューとして使われ、リスト区画４４０内に現在表示されているＩＰトンネル定義を示す。その小さいバー４３４あるいは第二の小さなバーも、照合した、またはほぼ照合しているトンネル定義が見つかるリスト内のエリアを示すために使用できる。

【００４８】リスト区画４４０は、ファイアウォールに対して定義した全てのＩＰトンネル定義のスクロール可能なリスト４４２を表示する。照合したＩＰトンネル定義は異なった色、または明るく点灯して表示される。管理者はエントリを選択して（または明るく点灯させて）それを編集したり、あるいはＩＰトンネル定義リストから削除する。読みやすくするため、ＩＰトンネル・エントリを縦列に分割し、全てのソース・アドレスが水平方向に並べられる。

【００４９】リスト・アクション区画４５０は、押しボタン４５２を作動させることにより管理者は、あるファイアウォールについての選択したＩＰトンネル定義のリストをロードすることが可能である。また、エントリ編集の押しボタン４５４を作動させることにより選択したＩＰトンネル定義を編集することが可能である。エントリ編集の押しボタン４５４を作動させることにより、ＩＰトンネル定義ページに表示した選択エントリの定義を有するＩＰトンネル定義ページに管理者を戻す。

【００５０】図７はＩＰトンネル／フィルタ照会ページを示す表示例である。このページは、あるインターネット。ファイアウォールについての２つの別な定義グループである、ＩＰトンネル定義およびＩＰフィルタ定義をまとめたものである。このＩＰフィルタ・グループは冒頭に明示した出願書類に説明されている。ＩＰトンネル画像ページに示したのと同じＩＰトンネル画像の選択に基づくＩＰフィルタ・ルールのリストに対して照会を管理者が行うことを可能とする。この画像５１２はディスプレイ区画５１０に示されている。画像のＩＰトンネル・ライン５１４およびディスプレイ・アクション区画の照会実行ボタン５２４を選択することは、ファイアウォール・フィルタ・ルールのリストにある照会を起こすことになる。ＩＰフィルタ・ルールはＩＰトンネル情報を含む必要がないが、管理者は、例えば、符号化を用いて定義したＩＰトンネルを通じて、特定のソース・アドレス、宛先アドレス、ポート番号から全てのＩＰパケットの経路を定めるための受け入れフィルタ・ルールを定義することができる。

【００５１】ディスプレイ・アクション区画５２０は管理者に２つのアクションの選択を提供する。すなわち、一方のボタン５２２はディスプレイ区画の明るく点灯しているＩＰトンネル選択をクリアし、もう一方のボタン５２４は選択したＩＰトンネル・ラインに基づくディスプレイ区画内で定義した照会を実行するためのものである。ディスプレイ・アクション区画もその選択したＩＰトンネルのＩＤ５２６、および照会テストで照合したＩＰフィルタ・ルールの番号を大きな字体で示す番号５２８を表示する。

【００５２】ＩＰトンネル照会ページでのように、メータ区画５３０はグラフィカル・バー５３２を表示するが、この場合には照合したＩＰフィルタ・ルールの分布を視覚的に示す。これらの照合したＩＰフィルタ・ルールはバーの他の部分とは異なる色で示される。このバー５３２は、視覚的かつ迅速に照合したＩＰフィルタ・ルールおよびＩＰフィルタ・ルール・リスト内の分布を示すので分散バーと呼ばれる。この分散バー５３２に隣接した小さなバー５３４が位置的キューとして使われ、リスト区画５４０内に現在表示されているＩＰフィルタ・ルールを示す。

【００５３】リスト区画５４０は、ファイアウォールに対して定義した全てのＩＰフィルタ・ルールのリスト５４２を表示する。管理者がＩＰトンネル定義を表すディスプレイ区画５１０内のライン５１４を選択すると、このウェブ・ページは、同じＩＰトンネルＩＤで定義されたリスト５４２内のＩＰフィルタ・ルール全てに色を着ける。照合したＩＰフィルタ・ルールは明るく点灯しているエントリとは逆に、異なった色で表示するのが望ましい。というのは、明るく点灯しているものはインターフェース内の選択用に使われるからである。管理者はこのリスト内のエントリを選択し、フィルタ・リストから編集することができる。

【００５４】リスト・アクション区画５５０は、フィルタ・リストのロードと示された押しボタン５５２を作動させることにより、管理者は、あるファイアウォールについてのＩＰフィルタ・ルールのリストをロードすることが可能である。また、編集エントリ押しボタン５５４を作動させることにより選択したＩＰフィルタ・ルールを編集することが可能である。フィルタ・ルールの編集については、フィルタ定義ページで引用した出願に説明されている。

【００５５】ＩＰトンネル・ページのデータ構造

【００５６】ＩＰトンネル・テーブル構造

ＩＰトンネル構造の数

ＩＰトンネル構造に対するポインタ
【００５７】ＩＰトンネル構造
トンネルＩＤ
目標アドレス
ローカル・アドレス
符号化アルゴリズム
セッション・キー寿命
セッション・キー再生時間
開始プログラム
立証ポリシィ
符号化ポリシィ
＜他の変数も各について作成可能＞
コメント
【００５８】ＩＰトンネル定義ページのデータ構造
修正したリスト区画の状態ビット
リスト区画のＩＰトンネル・テーブル構造
修正したディスプレイ区画の状態ビット
ディスプレイ区画のＩＰトンネル構造
【００５９】ＩＰトンネル画像ページのデータ構造
ディスプレイ区画のＩＰトンネル・テーブル構造
リスト区画ＩＰのトンネル・テーブル構造
一時ＩＰトンネル構造
【００６０】ＩＰトンネル照会ページのデータ構造
ディスプレイ区画のＩＰトンネル構造
ディスプレイ・アクション区画の照合トンネル数
メータ区画の上部区域
メータ区画の照合ＩＰトンネル・テーブル
リスト区画のＩＰトンネル・テーブル構造
一時ＩＰトンネル構造
【００６１】ＩＰトンネル／フィルタ照会ページのデータ構造
ディスプレイ区画のＩＰトンネル・テーブル構造
ディスプレイ・アクション区画の照合フィルタ数
メータ区画の上部区域
メータ区画の照合フィルタ・ルール・テーブル構造
リスト区画のフィルタ・ルール・テーブル構造
一時フィルタ・ルール構造
【００６２】上記のデータ構造はＩＰトンネル・テーブル構造を含んでいる。この構造はファイアウォールについて定義した全てのＩＰトンネルを保有する。ＩＰトンネル構造は単一のトンネル定義の全ての属性を表す。例えば、トンネル定義でのローカルおよび目標アドレスは、ＩＰトンネルの終点のソース装置および宛先ファイアウォール装置を確立するため使用される。別のＩＰトンネル属性は、そのＩＰトンネルを通るＩＰパケット用に確立された符号化アルゴリズムおよび立証ポリシィの種類を含む。
【００６３】ＩＰトンネル定義ページのデータ構造は、このページで情報のトラックを表示したり保存するために使用されたデータ構造を含む。修正したリスト区画の状態ビットは、トンネル定義が過去にこのインターフェースにロードされたのでＩＰトンネルのリストにトンネル定義が加えられたかどうか示す。リスト区画のＩＰトンネル・テーブル構造はそのファイウォールからロードされたトンネル定義の集合である。修正したディスプレイ区画の状態ビットは、管理者がそのディスプレイ区画で何らかの情報を変更したかどうか示す。ディスプレイ区画のＩＰトンネル構造はディスプレイ区画そのものに示された全ての値を保持する。
【００６４】ＩＰトンネル画像ページのデータ構造は、このページの情報のトラックを表示したり保持したりするため使用したデータ構造を含む。ディスプレイ区画のＩＰトンネル・テーブル構造はファイアウォールからロードしたトンネル定義の集合であり、この情報はこのページでトンネルを画像表示するため使用している。リスト区画ＩＰのトンネル・テーブル構造はファイアウォールからロードしたトンネル定義の集合である。一時ＩＰトンネル構造は、このページで管理者のアクションの結果として情報がＩＰトンネル定義ページに伝送される時に使用される選択ＩＰトンネル定義を保持するため使用されるものである。
【００６５】ＩＰトンネル照会ページのデータ構造は、このページで情報のトラックを表示したり保存するために使用されたデータ構造を含む。ディスプレイ区画のＩＰトンネル構造はディスプレイ区画そのものに表示した全ての値を保持する。ディスプレイ・アクション区画の照合トンネル数は、ディスプレイ区画でＩＰトンネルの照会明細と照合するインターフェースでロードされたトンネル定義の数である。メータ区画の上部区域はインターフェースでロードされたトンネル定義の数である。メータ区画の照合ＩＰトンネル・テーブルはディスプレイ区画でＩＰトンネルの照会明細と照合するインターフェースでロードされたトンネル定義の集合である。リスト区画のＩＰトンネル・テーブル構造はファイアウォールからロードされたトンネル定義の集合である。一時ＩＰトンネル構造は、このページで管理者のアクションの結果として情報がＩＰトンネル定義ページに伝送される時に使用される選択ＩＰトンネル定義を保持するため使用されるものである。
【００６６】ＩＰトンネル／フィルタ照会ページのデータ構造は、このページで情報のトラックを表示したり保存するために使用されたデータ構造を含む。ディスプレイ区画のＩＰトンネル・テーブル構造は、ファイアウォールからロードしたトンネル定義の集合であり、この情報はこのページでトンネルを画像表示するため使用している。ディスプレイ・アクション区画の照合フィルタ数は、ディスプレイ区画で選択されたＩＰトンネルＩＤと照合するインターフェースでロードしたＩＰフィルタ・ルールの数である。メータ区画の上部区域はインターフェースでロードされたフィルタ・ルールの数である。メ

ータ区画の照合フィルタ・ルール・テーブルはディスプレイ区画でＩＰトンネルのＩＤと照合するインターフェースでロードされたフィルタ・ルールの集合である。リスト区画のフィルタ・ルール・テーブル構造はファイアウォールからロードされたＩＰフィルタ・ルールの集合である。一時フィルタ・ルール構造は、このページで管理者のアクションの結果として情報がＩＰフィルタ定義ページに伝送される時に使用される選択フィルタ・ルールを保持するため使用されるものである。

【００６７】データの他の組合せを有する他のデータ構造が別の実施例で使用できることは、当業者が容易に理解できることである。

【００６８】図８には、ＩＰトンネル定義ページの表示区画におけるユーザ入力により本システムが行うプロセスを示す。このプロセスはステップ１０００で開始し、システムがユーザ入力を待ち受ける。ステップ１００５では、区画ボタンが押されたかどうか判定する。ＹＥＳならステップ１０１０で、組み合わせたエントリ・フィールドからの値がフェッチされる。ステップ１０１５は、組み合わせたエントリ・フィールドに値があるか判定する。ＮＯならば、システムはステップ１０００に戻る。ＹＥＳなら、ピン・ボタンのプログラムはステップ１０２０でその値についておこなわれる。そしてプロセスはステップ１０２５に進み、ピン・ボタンのプログラムの出力は命令が実行される間、メータ区画に送られる。管理者はこのようにしてピン・ボタンによる操作が成功したか失敗か、見ることができる。このプロセスはステップ１０００に戻り、ユーザの別のアクションを待機する。

【００６９】ステップ１００５の試験がＮＯなら、ステップ１０３０でトレースルート・ボタンが押されたか判定する。ＹＥＳならステップ１０３５で、組み合わせたエントリ・フィールドからの値がフェッチされる。ステップ１０４０は、組み合わせたエントリ・フィールドに値があるか判定する。ＮＯならば、システムはステップ１０００に戻る。ＹＥＳなら、トレースルート・ボタンのプログラムはステップ１０４５でその値についておこなわれる。そしてプロセスはステップ１０２５に進み、トレースルート・ボタンのプログラムの出力は命令が実行される間、メータ区画に送られる。このプロセスはステップ１０００に戻る。

【００７０】ステップ１０３０の試験がＮＯなら、ステップ１０５５で指ボタンが押されたか判定する。ＹＥＳならステップ１０６０で、組み合わせたエントリ・フィールドからの値がフェッチされる。ステップ１０６５は、組み合わせたエントリ・フィールドに値があるか判定する。ＮＯならば、システムはステップ１０００に戻る。ＹＥＳなら、指ボタンのプログラムはステップ１０７０でその値についておこなわれる。そしてプロセスはステップ１０２５に進み、指ボタンのプログラムの出力は命令が実行される間、メータ区画に送られる。このプロセスはステップ１０００に戻る。

【００７１】ステップ１０７５で指ボタンが押されてないなら、ディスプレイ区画のエントリが修正されたかどうか判定する。ＹＥＳなら、修正ビットをステップ１０８０でセットし、プロセスはステップ１０００に戻る。ＮＯならステップ１０８５でアクション理解不能とされ、このシステムは何も行わない。プロセスはステップ１０００に戻り、ユーザ入力を待つ。

【００７２】ＩＰトンネル定義ページの表示アクション区画のユーザ入力に応じて行われるプロセスが図９に示されている。ステップ１１００でプロセスが始まり、ユーザのアクションを待つ。ステップ１１０５では、クリア・ボタンが押されたか判定する。ＹＥＳなら、ステップ１１１０で、ディスプレイ区画修正ビットがセットされているか判定する。ＹＥＳなら、ステップ１１１５で、管理者はそのエントリを記憶させるか判断するように問われる。ＮＯであれば、ステップ１１２０において、ＩＰトンネル定義がディスプレイ区画から除去され、各フィールドは空白のままにされる。プロセスはステップ１１００に戻りユーザの別の入力を待つ。しかし、管理者がエントリを記憶させると指示すると、プロセスはステップ１１７７に進み、そこで値をディスプレイ区画で検証する。

【００７３】クリア・ボタンが押されてないなら、ステップ１１２５で、修正した選択エントリ・ボタンが押されているかどうか判定する。ＹＥＳなら、ステップ１１３０で、ディスプレイ区画の値を検証する。ステップ１１３５では、検証で間違いがあったかどうか判定するためのテストを実行する。ＹＥＳなら、ステップ１１４０で、その間違いをメータ区画に通知し、システムは１１００に戻り、ユーザの別なアクションを待つ。間違いがない、つまりＮＯならば、ステップ１１４５で、検証の成功がメータ区画に表示される。プロセスはステップ１１５０に進み、エントリがリスト区画で選択されたかどうか判定する。ＹＥＳならば、その選択されたエントリがディスプレイ区画からの値とリスト区画内で交換され、プロセスはステップ１１００に戻る。ＮＯならば、ステップ１１６０で同じＩＰトンネルＩＤを有するリスト・エントリがあるかどうか判定する。ＹＥＳならば、ステップ１１６５で、同じＩＤを有するＩＰトンネル・エントリはディスプレイ区画の値でリスト区画内において交換される。プロセスはユーザのアクションの待機を再開する。同じＩＰトンネルＩＤを有するエントリが無ければ、ステップ１１７０でディスプレイ区画の値がリスト区画の新たな列として加えられる。プロセスはステップ１１００に戻る。

【００７４】ステップ１１７５で、選択したエントリを加える、というボタンが押されたかどうか判定する。ＹＥＳならば、ステップ１１７７で、ディスプレイ区画の

値を検証する。ステップ１１８０では、検証で間違いがあったかどうか判定するためのテストを実行する。なんらかの間違いがあるなら、ステップ１１８５で、その間違いをメータ区画に通知し、システムは１１００に戻る。間違いがない、つまりＮＯならば、ステップ１１９０で、検証の成功がメータ区画に表示され、プロセスはステップ１１６０に進む。

【００７５】ステップ１１０５、１１２５、１１７５での判定テストが全て不成功なら、ステップ１１９５でアクション認識不能とされ、このシステムは何も行わない。プロセスはステップ１１００に戻り、ユーザ入力を待つ。

【００７６】図１０には、ＩＰトンネル定義ページのリスト区画におけるユーザ入力に応じたプロセスが示されている。ステップ１２００でプロセスが始まり、ユーザのアクションを待つ。ステップ１２０５では、リスト区画エントリが選択されたか判定する。ＹＥＳなら、ステップ１２１０で、ディスプレイ区画修正ビットがセットされているか判定する。ＹＥＳなら、ステップ１２１５で、管理者はそのエントリを記憶させるか判断するように問われる。ＮＯであれば、ステップ１２１３でリスト区画からの選択エントリとディスプレイ区画の内容が交換させられ、システムはステップ１２００に戻る。管理者がディスプレイ区画の値を記憶させると指示すると、プロセスはステップ１２２０に進み、そこでディスプレイ区画の値を検証する。ステップ１２２５では、検証で間違いがあったかどうか判定するためのテストを実行する。なんらかの間違いがあるなら、ステップ１２３０で、その間違いをメータ区画に通知し、システムは１２００に戻る。間違いがない、つまりＮＯならば、ステップ１２３５で、検証の成功がメータ区画に表示され、プロセスはステップ１２４０に進む。ステップ１２４０では、ディスプレイ・ページからのと同じトンネルＩＤを有するリスト・エントリがあるか判定する。あるなら、ステップ１２４５でＩＰトンネル・エントリはリスト区画でディスプレイ区画値を有する同じＩＤと交換される。この場合、管理者は既に存在するトンネル定義を修正している。ステップ１２４０の判定がＮＯなら、ステップ１２５０でディスプレイ区画の値がリスト区画内の新たな列として加えられる。

【００７７】ステップ１２０５でＮＯなら、ステップ１２５５でアクション認識不能とされ、処理はステップ１２００に続く。

【００７８】図１１、図１２には、ＩＰトンネル定義ページのリスト・アクション区画におけるユーザ入力によって行われるプロセスを示す。ステップ１３００でプロセスが始まり、ユーザの入力を待つ。ステップ１３０３では、エントリ削除ボタンが押されたか判定する。ＹＥＳなら、ステップ１３０５で、エントリがリスト区画で選択されたか判定する。ＮＯなら、システムはステップ１３００に戻りユーザの別の入力を待つ。エントリがステップ１３１０で選択されたなら、リスト区画からその選択エントリを除去する。ステップ１３１３で、エントリの削除がＩＰトンネル定義ページのメータ区画に通知される。プロセスはステップ１３００に戻る。

【００７９】ステップ１３１５では、エントリ活性化ボタンが押されたか判定する。ＹＥＳなら、ステップ１３２０で、エントリがリスト区画で選択されたか判定する。ＮＯなら、システムはステップ１３００に戻る。エントリがステップ１３２５で選択されたなら、選択したＩＰトンネル・エントリの活性属性を活性にセットする。プロセスはステップ１３００に戻りユーザのアクションを待つ。活性トンネルとは、ＩＰトンネルを通じてパケットと照合する経路をつくるためにフィルタ・ルールが定義されている時、ファイアウォールが複数のＩＰパケットを送ることのできるものである。ＩＰトンネルは定義可能であるが、複数のＩＰパケットを受けいれるために活性にはできない。

【００８０】ステップ１３３０では、エントリ不活性化ボタンが押されたか判定する。ＹＥＳなら、ステップ１３３３で、エントリがリスト区画で選択されたか判定する。ＮＯなら、システムはステップ１３００に戻りユーザのアクションを待つ。エントリがステップ１３３５で選択されたなら、選択したＩＰトンネル・エントリの活性属性を不活性化にセットする。プロセスはステップ１３００に戻りユーザのアクションを待つ。

【００８１】ステップ１３３９では、からロードというボタンが押されたか判定する。ＹＥＳなら、ステップ１３４０で、管理者はどのファイアウォールからＩＰトンネル定義をロードするか問われる。ステップ１３４５で、特定のファイアウォールからのＩＰトンネル定義がロードされる。ステップ１３５０では、ロード処理で誤りがあるかどうか判定する。誤りがあるなら、ステップ１３５５で、誤りをメータ区画に通知する。誤りがないなら、ステップ１３６０で、ロード処理の成功をメータ区画に通知する。ステップ１３６５では、リスト区画エントリはロードしたＩＰトンネル・リストと交換される。ステップ１３６９では、ディスプレイ区画エントリはクリアされる。ステップ１３７０では、ディスプレイ区画修正ビットがセット・オフされる。プロセスはステップ１３００に戻りユーザの入力を待つ。

【００８２】ステップ１３７３では、ファイアウォールへ保存というボタンが押されたか判定する。ＹＥＳなら、ステップ１３７５で、管理者はどのファイアウォールへＩＰトンネル定義を保存するか問われる。ステップ１３７７で、特定されたファイアウォールへＩＰトンネル定義を保存する。ステップ１３７９では、保存の結果をメータ区画に通知する。プロセスはステップ１３００に戻る。

【００８３】図１３では、ステップ１３８０において、

ファイアウォール活動停止というボタンが押されたか判定する。このボタンが押されたなら、ステップ１３８５でファイアウォールの全てのＩＰトンネル定義は停止あるいは不活性とされる。ステップ１３８７で、停止の結果をメータ区画に通知する。

【００８４】ステップ１３９０で、ファイアウォール間で検証というボタンが押されたか判定する。このボタンが押されたなら、ステップ１３９３でファイアウォール間、つまりソースファイアウォールと目標ファイアウォール間のトンネル定義をＩＰトンネル・リストで検証される。検証プロセスはファイアウォールにより提供されたものと同じである。ステップ１３９７で、システムはこのアクションは理解不能であると判定し、何も行わない。この時点で、プロセスはステップ１３００に戻り、ユーザの別な入力を待つ。

【００８５】ＩＰトンネル画像ページの表示アクション区画のユーザ入力に応じて行われるシステム・アクションを図１４に示している。ステップ１４００でプロセスが始まり、ユーザの入力を待つ。ステップ１４０５では、全てを見せるというボタンが押されたか判定する。ＹＥＳなら、ステップ１４１０で、ディスプレイ区画の画像が書き直され、全てのＩＰトンネルを見せる。ステップ１４１５０では、活動中のものを見せるというボタンが押されたか判定する。ＹＥＳなら、ステップ１４２０で、ディスプレイ区画で画像が書き直され、活動中のＩＰトンネル接続を明るく点灯する。プロセスはステップ１４００に戻る。ステップ１４２５で、非活動中のものを見せるというボタンが押されたか判定する。ＹＥＳなら、ステップ１４２３で、ディスプレイ区画で画像が書き直され、非活動中のＩＰトンネル接続を明るく点灯する。ステップ１４３５で、このシステムはユーザ入力が不明のアクションとして分類し、ステップ１４００に戻りユーザの別な入力を待つ。

【００８６】図１５、図１６はＩＰトンネル画像ページにおけるリスト・アクション区画の入力からのシステム・アクションを示す。ステップ１５００でプロセスが始まり、ユーザの入力を待つ。ステップ１５０３では、エントリ編集ボタンが押されたか判定する。ＹＥＳなら、ステップ１５０５で、エントリがリスト区画で選択されたか判定する。ＮＯなら、システムはステップ１５００に戻りユーザの別の入力を待つ。エントリがステップ１５０７で選択されたなら、その選択エントリの内容を一時ＩＰトンネル定義構造に記憶させる。ステップ１５０９で、ＩＰトンネル定義ページが表示される。ステップ１５１０で、一時ＩＰトンネル定義の内容がディスプレイ区画に表示され、プロセスは図１１、図１２、図１３、図１４、図１５、図１６に示したＩＰトンネル定義ページのアクションに進む。

【００８７】ステップ１５１５では、エントリ削除ボタンが押されたか判定する。ＹＥＳなら、ステップ１５１７で、エントリがリスト区画で選択されたか判定する。ＮＯなら、システムはステップ１５００に戻りユーザの別の入力を待つ。エントリがステップ１５１７で選択されたなら、ステップ１５１９でリスト区画からその選択エントリを除去し、ステップ１５２０ではリスト区画修正ビットをセット・オンする。ステップ１５２３では、ＩＰトンネル画像が描き直され、リスト区画の新しい内容を反映させる。プロセスはステップ１５００に戻る。

【００８８】ステップ１５２５では、エントリ活性化ボタンが押されたか判定する。ＹＥＳなら、ステップ１５２９で、エントリがリスト区画で選択されたか判定する。エントリが選択されたなら、選択したエントリのＩＰトンネル定義をステップ１５３０で活性化し、プロセスはステップ１５２０にもどる。

【００８９】ステップ１５３５で、エントリ不活性化ボタンが押されたか判定する。ＹＥＳなら、ステップ１５３９で、エントリがリスト区画で選択されたか判定する。エントリが選択されたなら、選択したエントリのＩＰトンネル定義をステップ１５４０で不活性化し、プロセスはステップ１５２０にもどり、リスト区画修正ボタンをセットし、ステップ１５２３でＩＰトンネル画像を描き直す。

【００９０】ステップ１５４５では、ファイアウォールからロードというボタンが押されたか判定する。ＹＥＳなら、ステップ１５５０で、リスト区画修正ビットがオンか判定する。ＮＯであれば、ステップ１５５３で、管理者はどのファイアウォールからロードするか問われる。ステップ１５５５で、特定したファイアウォールからのＩＰトンネル定義がロードされる。ステップ１５６０では、ロード処理で誤りがあるかどうか判定する。誤りがあるなら、ステップ１５６３で、誤りをチッカ・テープ区画に通知し、プロセスはステップ１５００に戻る。誤りがないなら、ステップ１５６５で、ロード処理の成功をチッカ・テープ区画に通知する。ステップ１５７０では、リスト区画のＩＰトンネルリストをロードしたＩＰトンネル・リストと交換する。ステップ１５７３では、リスト区画修正ビットがセット・オフされる。プロセスはステップ１５２３に戻り、ＩＰトンネル画像がディスプレイ区画で描き直される。

【００９１】ステップ１５７５では、管理者は現在のリスト区画内容を保存するか問われる。管理者がそのリスト区画内容を保存すると指示したら、ステップ１５８０で、その内容が目標ファイアウォールのＩＰトンネル・テーブルとして保存される。ステップ１５８３では、その結果をチッカ・テープ区画に通知する。この時点で、プロセスはステップ１５５３に戻り、管理者にどのファイアウォールからロードするか問う。

【００９２】図１７のステップ１５８５では、ファイアウォールへ保存というボタンが押されたか判定する。ＹＥＳなら、ステップ１５９０で、管理者はどのファイア

ウォールへ保存するか問われる。ステップ１５９３で、特定したファイアウォールへリスト区画のＩＰトンネル定義を保存する。ステップ１５９５では、保存の結果をチッカ・テープ区画に通知する。プロセスはステップ１５００に戻りユーザの入力を待つ。ステップ１５９７で、このアクションは不明アクションとして分類され、プロセスはステップ１５００に戻りユーザの入力を待つ。

【００９３】図１８はＩＰトンネル照会ページの表示アクション区画におけるユーザ入力により行われるシステム・アクションを示すフローチャートである。ステップ１６００でプロセスが始まり、ユーザの入力を待つ。ステップ１６０５では、クリア・ボタンが押されたか判定する。ＹＥＳなら、ステップ１６１０で、ＩＰトンネル値がディスプレイ区画から除去される、つまりエントリ・フィールドは空白である。ステップ１６１５では、メータ区画のリンクしたリストがクリアされ、メータ区画が表示される。ステップ１６２０では、チッカ・テープ区画がクリアされる。ステップ１６２５では、ディスプレイ・アクション区画で照合した数としてゼロが表示される。プロセスはステップ１６００に戻り、ユーザのアクションを待つ。

【００９４】ステップ１６３０では、照会実行ボタンが押されたか判定する。押されたなら、ステップ１６３５で、メータ区画リンク・リストがクリアされ、ＩＰトンネル・テーブルを介してカウンタを増加するため使用する変数ｉを１にセットする。ステップ１６４０では、ｉがＩＰトンネル・テーブルのＩＰトンネルの数より大きいか判定する。大きくないなら、ステップ１６４５でＩＰトンネル・テーブルがＩＰトンネル・エントリの照会明細と照合しているか判定する。これはリスト区画の指標列に対してディスプレイ区画の入力を照合させることにより行われる。ステップ１６５０では、ｉによる指標のＩＰトンネル・テーブルはメータ区画リンク・リストに加えられる。ステップ１６５５では、ｉが１増加し、プロセスはステップ１６４０に戻る。ｉがＩＰトンネル・テーブルのＩＰトンネルの数を越えるなら、ステップ１６６０ではメータ区画リンク・リストがエントリを有するか判定する。ＹＥＳなら、ステップ１６６５において、照合するエントリにメータ区画内で陰影を着ける。結果をチッカ・テープ区画ステップ１６７０に表示し、ステップ１６７５では、照合した数をディスプレイ・アクション区画に表示する。プロセスはステップ１６００に戻りユーザのアクションを待つ。ステップ１６８０では、このアクションは認識されず、プロセスはステップ１６００に戻る。

【００９５】図１９では、ＩＰトンネル照会ページのリスト区画に対するユーザ入力に応じて行うシステム・アクションを示す。ステップ１７００でユーザ入力を待つ。ステップ１７０５では、エントリが選択されたか判定する。選択されたなら、ステップ１７１０で、エントリをディスプレイ区画で交換する。ディスプレイ・アクション照合数はステップ１７１５で「ゼロ」に変わる。次に、ステップ１７２０で、メータ区画リンク・リストがクリアされ、メータ区画での陰影もクリアされる。ステップ１７００に戻り、ユーザ・アクションを待つ。

【００９６】ステップ１７２５では、リストがリスト区画でスクロールされたか判定する。ＹＥＳなら、ステップ１７３０でメータ区画の位置キューの垂直バーがリスト区画で示されているものと照合するように変えられる。プロセスはステップ１７００に戻る。ステップ１７３５では、このアクションは不明とされ、何も行わない。そして、ステップ１７００に戻り、ユーザのアクションを待つ。

【００９７】ＩＰトンネル照会ページのリスト・アクション区画におけるユーザ入力に応じたシステムのアクションが図２０に示されている。ステップ１８００で、ユーザ入力を待つ。ステップ１８０５では、編集ボタンが押されたか判定する。ＹＥＳなら、ステップ１８１０で、リスト区画にエントリがあるか、またそれは選択されたか判定される。ＮＯならば、システムはステップ１８００に戻る。ＹＥＳなら、ステップ１８１５で、選択エントリの内容を一時ＩＰトンネル定義構造に記憶させる。ステップ１８２０で、ＩＰトンネル定義ページが表示され、ステップ１８２５で、一時ＩＰトンネル定義構造の内容がディスプレイ区画に置かれる。次に、システムはステップ１８３０の図１０、１１、１２、１３、１４、１５、１６に関連して説明したＩＰトンネル定義ページ・アクションに進む。

【００９８】ステップ１８３５で、ＩＰトンネルをロードするというボタンが押されたか判定する。ＹＥＳなら、ステップ１８４０で、ファイアウォールから記憶させたＩＰトンネル定義をロードする。ステップ１８４５で、新たなＩＰトンネル・テーブルをリスト区画に表示する。プロセスはステップ１８００に戻る。

【００９９】ステップ１８５０で、このアクションは認識せずと判定し、何も行わない。プロセスはステップ１８００に戻り、ユーザ入力を待つ。

【０１００】図２１は、ＩＰトンネル／フィルタ照会ページの表示アクション区画におけるユーザ入力に応じたシステム・アクションを示す。ステップ１９００で、ユーザ入力を待つ。ステップ１９０５で、クリア・ボタンが押されたか判定する。ＹＥＳなら、ステップ１９１０で、明るい点灯を画像およびディスプレイ区画から除去する。ステップ１９１５で、メータ区画リンク・リストはクリアされ、メータ区画が再度表示される。ステップ１９２０で、チッカ・テープ区画がクリアされる。ステップ１９２５で、ディスプレイ・アクション区画で照合したフィルタの数としてゼロが表示され、選択したＩＰトンネルの数が表示され、プロセスはステップ１９００

に戻る。

【０１０１】ステップ１９３０で、照会実行のボタンが押されたか判定する。押されたのなら、ステップ１９３５で、メータ区画リンク・リストがクリアされ、変数ｉを１にセットする。ステップ１９４０では、ｉがリスト区画のＩＰフィルタ・ルールの数より大きいか判定する。大きくないなら、ステップ１９４５でＩＰフィルタ・テーブルが、ディスプレイ区画で選択ＩＤトンネルと照合するトンネルＩＤを有するか判定する。ＹＥＳなら、ステップ１９５０で、ＩＰフィルタ・テーブルのｉによる指標のトンネル定義がメータ区画リンク・リストに加えられる。ステップ１９５５では、変数ｉが増加させられる。

【０１０２】ステップ１９６０で、メータ区画リンク・リストがエントリを有するか判定する。ＹＥＳなら、ステップ１９６５において、照会定義と照合するメータ・リスト・エントリにメータ区画内で陰影を着ける。１９７０で、結果をチッカ・テープ区画に表示し、ステップ１９７５では、フィルタと照合した数をディスプレイ・アクション区画に表示する。プロセスはステップ１９００に戻る。

【０１０３】ステップ１９８０では、このアクションは認識されず、プロセスはステップ１９００に戻り、ユーザの別なアクションを待つ。

【０１０４】図２２は、ＩＰトンネル／フィルタ照会ページのリスト区画へのユーザ入力によるシステム・アクションを示す。ステップ２０００で、ユーザ入力を待つ。ステップ２００５で、エントリが選択されたか判定する。ＹＥＳなら、ステップ２０１０でディスプレイ・アクション照合数が「ゼロ」に変わる。選択したＩＰトンネルをディスプレイ・アクション区画から除去する。ステップ２０１５では、メータ区画リンク・リストがクリアされ、メータ区画を再度表示する。ステップ２０２０では、明るい点灯をディスプレイ区画の選択エントリから除去する。

【０１０５】ステップ２０２５では、リストがスクロールされたか判定する。ＹＥＳなら、ステップ２０３０で、メータ区画の垂直バーの位置キューを、リスト区画に示されているものと照合するように変える。ステップ２０３５では、このアクションは不明とする。プロセスはステップ２０００に戻り、ユーザ入力を待つ。

【０１０６】図２３は、ＩＰトンネル／フィルタ照会ページのリスト・アクション区画に対するユーザ入力に応じたシステム・アクションを示す。ステップ２１００で、ユーザ入力を待つ。ステップ２１０５で、エントリ編集ボタンが押されたか判定する。ＹＥＳなら、ステップ２１１０でリスト区画のエントリが選択されたか判定する。ＮＯなら、システムはステップ２１００に戻り、ユーザ・アクションを待つ。ステップ２１１５では、選択したエントリの内容を一時ＩＰフィルタ・ルール構造に記憶する。ステップ２１２０で、ＩＰフィルタ定義ページが表示される。ステップ２１２５では、一時ＩＰフィルタ・ルール構造の内容をディスプレイ区画に表示し、ステップ２１３０では前述の引例に説明があるＩＰフィルタ定義ページ・アクションに進む。

【０１０７】ステップ２１３５では、フィルタ・リストをロードするというボタンが押されているか判定する。ＹＥＳなら、ステップ２１４０でファイアウォールからのこれらのＩＰ／フィルタ定義を記憶させる。ステップ２１４５では、新たなＩＰフィルタ・テーブルをリスト区画に示す。ステップ２１５０では、このアクションは不明とし、アクションはとらない。プロセスはステップ２１００に戻る。

【０１０８】上記の説明はＩＰトンネリングおよびフィルタ処理、つまり種々のインターネット本体により公表されたトンネル・ルールおよびフィルタ・ルールに関するものであり、本発明は安全なネットワークと安全でないネットワーク間に課することの可能なトンネル・ルールとフィルタ・ルールの集合への応用である。例えば、マイクロソフト社によって初め提案されたポイント対ポイント・トンネリング・プロトコルは、本発明の使用により最小限の改修で管理可能となる。

【０１０９】本発明の特定の実施例について示し、説明を行ったが、本発明が修正により他の環境においても実施可能であることは当業者に容易に理解されるであろう。例えば、上記説明の本発明は選択的に改変したりソフトウェアにより作動させた、汎用コンピュータにおいて容易に実行可能であるが、本発明はハードウェア、ファームウェア、あるいはソフトウェア、ファームウェアまたは上記の本発明を実現するため特別設計した特殊な装置を含むハードウェアのいかなる組合せでも実行可能であることは、当業者は容易に理解できる。従って、形態および細部の変更は前述の請求の範囲の精神および範囲を逸脱しない限り、行えるものである。

【０１１０】まとめとして、本発明の構成に関して以下の事項を開示する。

【０１１１】（１）安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータにおけるトンネリングを管理する方法において、複数のネットワークのアドレス間のトンネルのグラフィック図をネットワーク・アドレスを示すアイコンを接続するラインとして表示するステップと、第一ラインのユーザの選択に応じて、その第一ラインによって示された選択したトンネル定義を表示するステップと、ユーザ入力に応じて、上記選択したトンネル定義へのアクションを行うステップとを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理する方法。

（２）上記トンネルのグラフィック図は、ユーザ入力により、全ての定義したトンネルを示し、活動中のトンネ

ルを示し、あるいは非活動中のトンネルを示すように選択的に変えることが可能であることを特徴とする、上記（１）に記載の方法。

（３）上記ラインは、各々のトンネルの特性を示す異なった方法で描かれていることを特徴とする、上記（１）に記載の方法。

（４）上記特性はトンネルに可能な安全状態であることを特徴とする、上記（３）に記載の方法。

（５）上記グラフィック図は各トンネルが発生してくる方向を示す印を有することを特徴とする、上記（１）に記載の方法。

（６）安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理する方法において、トンネル定義を入れることのできる第一区画を有するユーザ・インターフェースを示すステップと、ユーザ入力に応じて、入力されたトンネル定義と既存のトンネル定義が照合するか判定するために、入力されたトンネル定義についての照会を実行するステップと、上記照会の結果を分散バーでユーザ・インターフェースの別な区画に表示し、トンネル定義の照合の位置は分散バーを通るラインにより示されるステップと、ユーザ入力に応じて、選択トンネル定義についてのアクションを行うステップとを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理する方法。

（７）第三区画でトンネル定義のリストを表示し、そこでは照合するトンネル定義が照合しないトンネル定義とは異なった方法で表示するステップと、上記分散バーに隣接し、上記分散バーによって示されたトンネル定義の完全なリストに関して第三区画に表示したトンネル定義のリストの位置を示す小さなバーを表示するステップとを、さらに有することを特徴とする上記（６）に記載の方法。

（８）上記分散バーに隣接し、照合するトンネル定義の集中を示す小さなバーを表示するステップを、さらに有することを特徴とする上記（６）に記載の方法。

（９）安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理する方法において、複数のネットワークのアドレス間のトンネルのグラフィック図をネットワーク・アドレスを示すアイコンを接続するラインとして表示するステップと、第一ラインのユーザの選択に応じて、その第一ラインによって示された選択したトンネルに応用できるフィルタ・ルールのリストを表示するステップと、ユーザ入力に応じて、上記選択したフィルタ・ルールへのアクションを行うステップとを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理する方法。

（１０）ユーザ入力に応じて、選択したトンネルに既存のフィルタ・ルールが応用可能か判定するために、選択したトンネルについての照会を実行するステップと、上記照会の結果を分散バーでユーザ・インターフェースの別な区画に表示し、フィルタ・ルールの照合の位置は分散バーを通るラインにより示されるステップとを更に有することを特徴とする、上記（９）に記載の方法。

（１１）照合するフィルタ・ルールを、フィルタ・ルールのリストの照合しないフィルタ・ルールとは異なった方法で表示するステップと、上記分散バーに隣接し、上記分散バーによって示されたフィルタ・ルールの完全なリストに関して第三区画に表示したフィルタ・ルールのリストの位置を示す小さなバーを表示するステップとを、さらに有することを特徴とする上記（１０）に記載の方法。

（１２）安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理するためのプロセッサとメモリを有するシステムにおいて、複数のネットワークのアドレス間のトンネルのグラフィック図をネットワーク・アドレスを示すアイコンを接続するラインとして表示する手段と、第一ラインのユーザの選択に応じて、その第一ラインによって示された選択したトンネル定義を表示する手段と、ユーザ入力に応じて、上記選択したトンネル定義へのアクションを行う手段とを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理するシステム。

（１３）上記トンネルのグラフィック図は、ユーザ入力により、全ての定義したトンネルを示し、活動中のトンネルを示し、あるいは非活動中のトンネルを示すように選択的に変えることが可能であることを特徴とする、上記（１２）に記載のシステム。

（１４）上記ラインは、各々のトンネルの特性を示す異なった方法で描かれていることを特徴とする、上記（１２）に記載のシステム。

（１５）上記特性はトンネルに可能な安全状態であることを特徴とする、上記（１４）に記載のシステム。

（１６）上記グラフィック図は各トンネルが発生してくる方向を示す印を有することを特徴とする、上記（１２）に記載のシステム。

（１７）安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理するためのプロセッサとメモリを有するシステムにおいて、トンネル定義を入力することのできる第一区画を有するユーザ・インターフェースを示す手段と、ユーザ入力に応じて、入力されたトンネル定義と既存のトンネル定義が照合するか判定するために、入力されたトンネル定義についての照会を実行する手段と、上記照会の結果を分散バーでユーザ・インターフェースの別な区画に表示し、トンネル定義の照合の位置は分散バーを通るラインにより示される手段と、ユーザ入力に応じて、選択トンネル定義について

のアクションを行う手段とを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理するシステム。

（１８）第三区画でトンネル定義のリストを表示し、そこでは照合するトンネル定義が照合しないトンネル定義とは異なった方法で表示する手段と、上記分散バーに隣接し、上記分散バーによって示されたトンネル定義の完全なリストに関して第三区画に表示したトンネル定義のリストの位置を示す小さなバーを表示する手段とを、さらに有することを特徴とする上記（１７）に記載のシステム。

（１９）上記分散バーに隣接し、照合するトンネル定義の集中を示す小さなバーを表示する手段を、さらに有することを特徴とする上記（１７）に記載のシステム。

（２０）安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理するプロセッサとメモリを有するシステムにおいて、複数のネットワークのアドレス間のトンネルのグラフィック図をネットワーク・アドレスを示すアイコンを接続するラインとして表示する手段と、第一ラインのユーザの選択に応じて、その第一ラインによって示された選択したトンネルに応用できるフィルタ・ルールのリストを表示する手段と、ユーザ入力に応じて、上記選択したフィルタ・ルールへのアクションを行う手段とを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理するシステム。

（２１）ユーザ入力に応じて、選択したトンネルに既存のフィルタ・ルールが応用可能か判定するために、選択したトンネルについての照会を実行する手段と、上記照会の結果を分散バーでユーザ・インターフェースの別な区画に表示し、フィルタ・ルールの照合の位置は分散バーを通るラインにより示される手段とを更に有することを特徴とする、上記（２０）に記載の方法。

（２２）照合するフィルタ・ルールを、フィルタ・ルールのリストの照合しないフィルタ・ルールとは異なった方法で表示する手段と、上記分散バーに隣接し、上記分散バーによって示されたフィルタ・ルールの完全なリストに関して第三区画に表示したフィルタ・ルールのリストの位置を示す小さなバーを表示する手段とを、さらに有することを特徴とする上記（２１）に記載の方法。

【図面の簡単な説明】

【図１】本発明により構成されたコンピュータ・システムの構成図である。

【図２】本発明が使用される環境の一実施例を示す概略図である。

【図３】本発明が使用される環境の別の実施例を示す概略図である。

【図４】ウェブ・ベースのユーザ・インターフェースにおけるＩＰトンネル定義のページを示す表示例。

【図５】ウェブ・ベースのユーザ・インターフェースにおけるＩＰトンネルのグラフィック・ページを示す表示例。

【図６】ユーザ・インターフェースにおけるＩＰトンネル照会ページを示す表示例。

【図７】ユーザ・インターフェースにおけるＩＰトンネル／フィルタ照会ページを示す表示例。

【図８】ＩＰトンネル定義ページの表示区画とアクションを示すフローチャート。

【図９】ＩＰトンネル定義ページの表示アクション区画のアクションを示すフローチャート。

【図１０】ＩＰトンネル定義ページのリスト区画におけるユーザ入力に従うアクションを示すフローチャート。

【図１１】ＩＰトンネル定義ページのリスト・アクション区画におけるユーザ入力によって取るアクションを示すフローチャートの前半部分。

【図１２】図１１のフローチャートの後半部分。

【図１３】図１２に続くフローチャート。

【図１４】ＩＰトンネル画像ページの表示アクション区画のユーザ入力に応じるプロセスを示すフローチャート。

【図１５】ＩＰトンネル画像ページにおけるリスト・アクション区画の入力からのシステム・アクションを示すフローチャートの前半部分。

【図１６】図１５のフローチャートの後半部分。

【図１７】図１６に続くフローチャート。

【図１８】ＩＰトンネル照会ページの表示アクション区画におけるユーザ入力により取られるシステム・プロセスを示すフローチャート。

【図１９】ＩＰトンネル照会ページのリスト区画における入力により取られるアクションを示すフローチャート。

【図２０】ＩＰトンネル照会ページのリスト・アクション区画におけるユーザ・アクションに応じたシステムのアクションを示すフローチャート。

【図２１】ＩＰトンネル／フィルタ照会ページの表示アクション区画における入力に応じたシステム・アクションを示すフローチャート。

【図２２】ＩＰトンネル／フィルタ照会ページのリスト区画から取られるアクションを示すフローチャート。

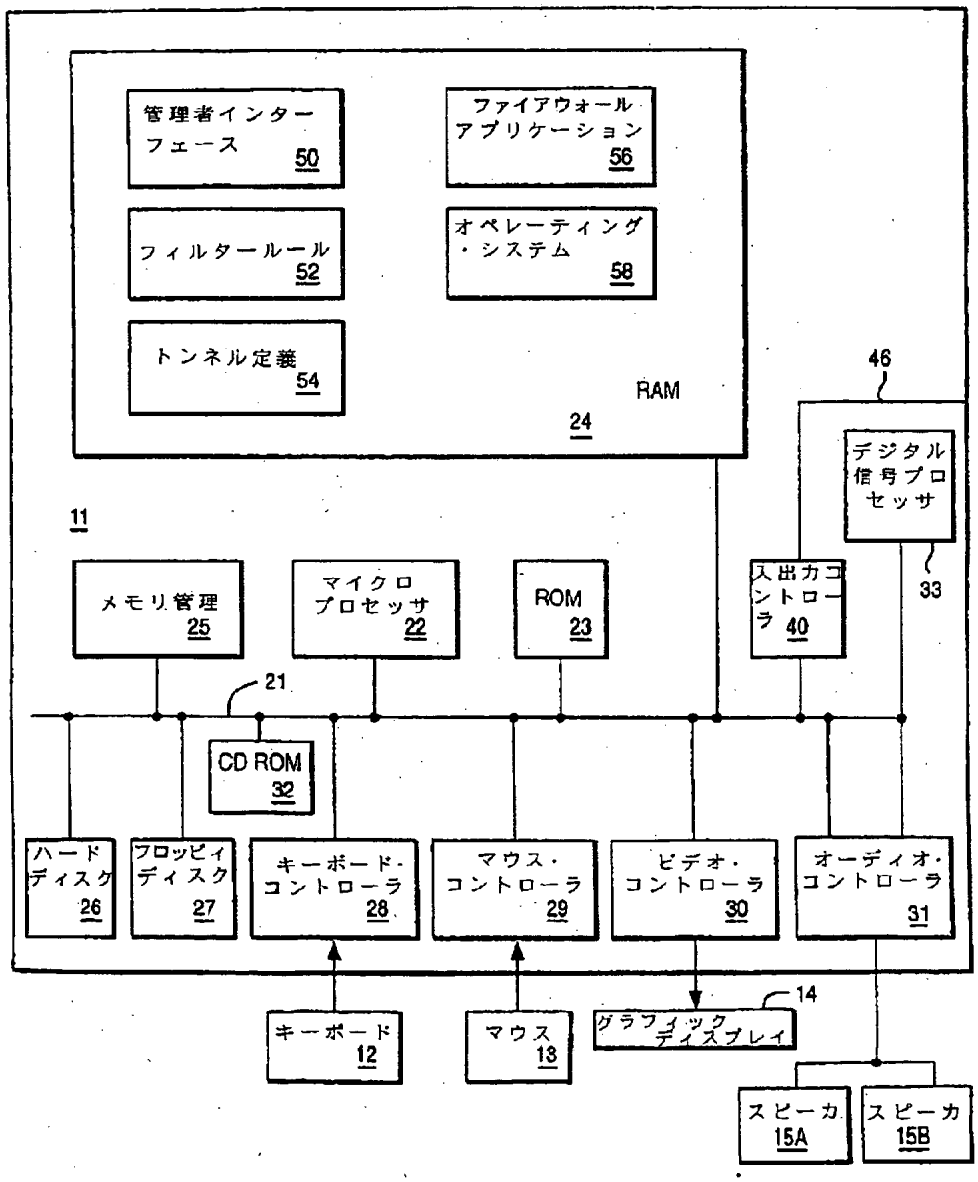
【図２３】ＩＰトンネル／フィルタ照会ページのリスト・アクション区画におけるユーザ・アクションに応じたシステム・アクションを示すフローチャート。

【符号の説明】

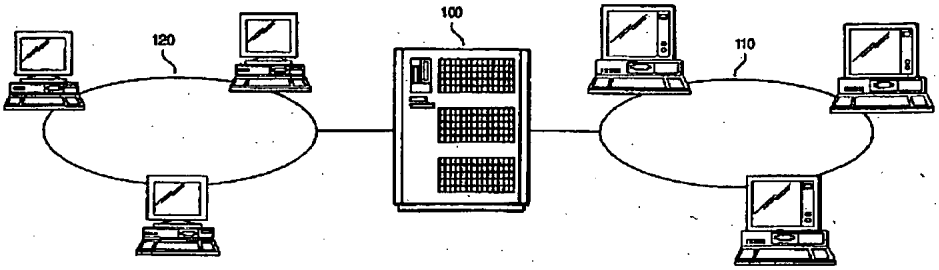
１１　システム・ユニット
１２　キーボード
１３　マウス
１４　ディスプレイ
２１　システム・バス
２２　マイクロプロセッサ

２３　読取り専用メモリ（ＲＯＭ）
２４　ランダム・アクセス・メモリ（ＲＡＭ）
２５　メモリ管理チップ
２６　ハード・ディスク・ドライブ
２７　フロッピイ・ディスク・ドライブ
２８　キーボード・コントローラ
２９　マウス・コントローラ
３０　ビデオ・コントローラ
３１　オーディオ・コントローラ
３２　ＣＤ-ＲＯＭ
４０　入力／出力コントローラ
２００　ナビゲーション区画
２１０　ディスプレイ区画
２１２　エントリ・フィールド
２１４　押しボタン
２１６　スクロール・バー
２２０　ディスプレイ・アクション区画
２３０　メータ区画
２４０　リスト区画
２４４　スクロール・バー
２４６　スクロール・バー
２５０　リスト・アクション区画
２５２　押しボタン
２６０　チッカ・テープ区画

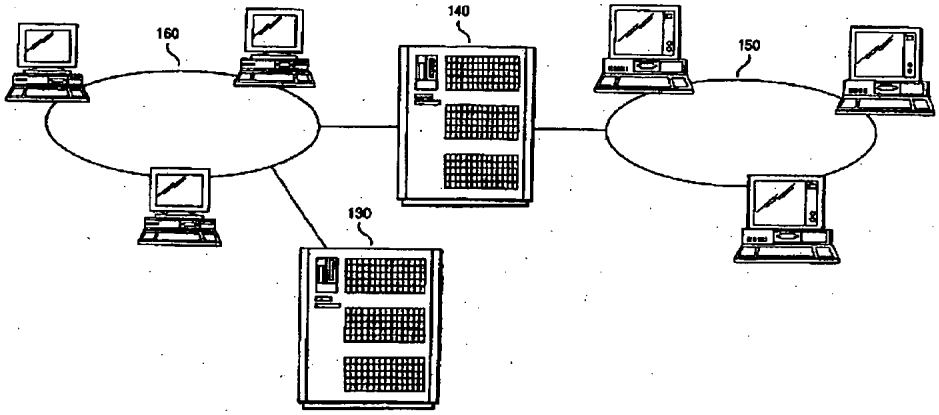
【図１】



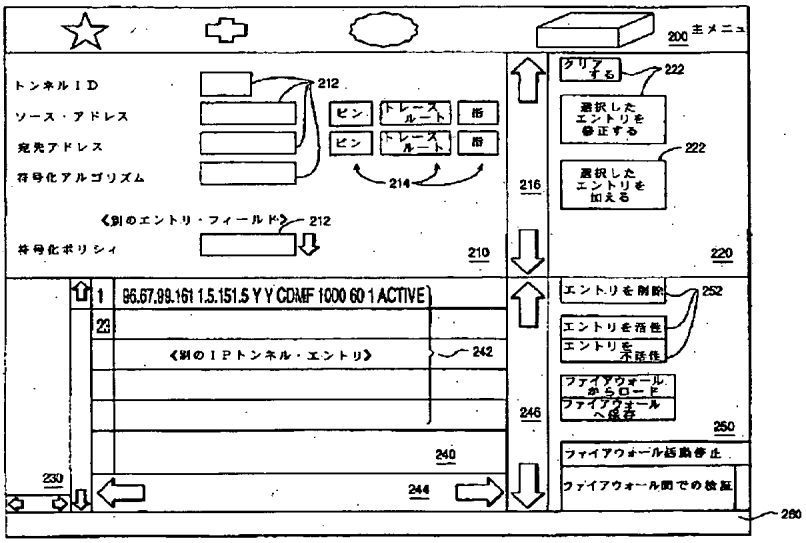
【図２】


100
110
120

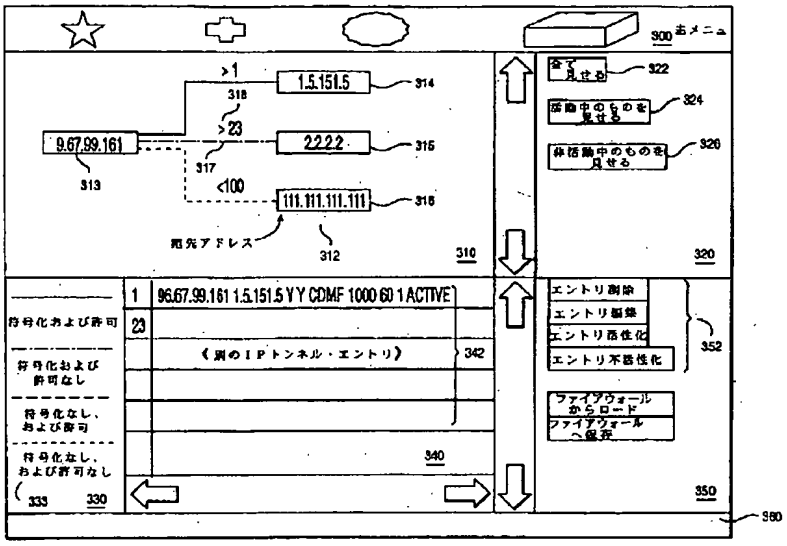
【図３】


130
140
150
160

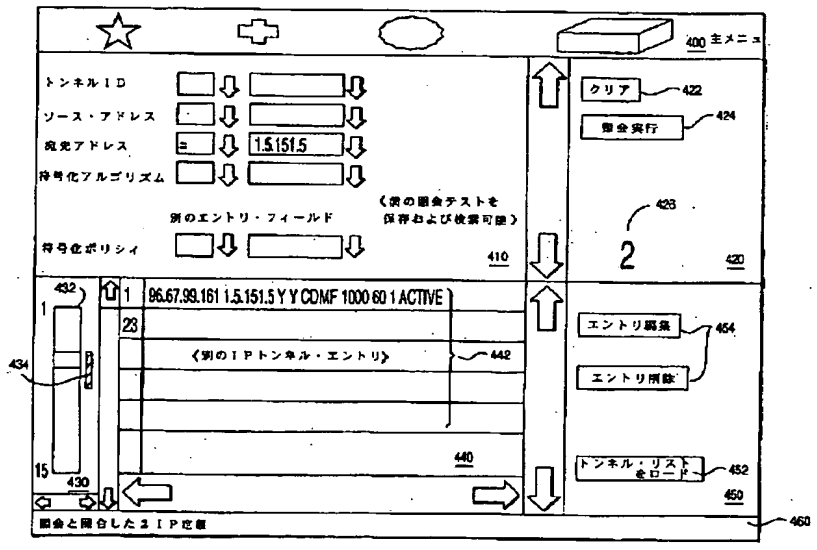
【図４】


200 主メニュー
トンネルＩＤ
ソース・アドレス
宛先アドレス
符号化アルゴリズム
212
ビン
トレース・ルート
指
214
《別のエントリ・フィールド》
符号化ポリシィ
210
クリアする
222
選択したエントリを修正する
選択したエントリを加える
216
220
エントリを削除
252
エントリを活性
エントリを不活性
ファイアウォールからロード
ファイアウォールへ保存
246
250
ファイアウォール活動停止
ファイアウォール間での検証
1 86.67.99.161 1.5.151.5 Y Y CDMF 1000 60 1 ACTIVE
23
《別のＩＰトンネル・エントリ》
242
240
230
244
260

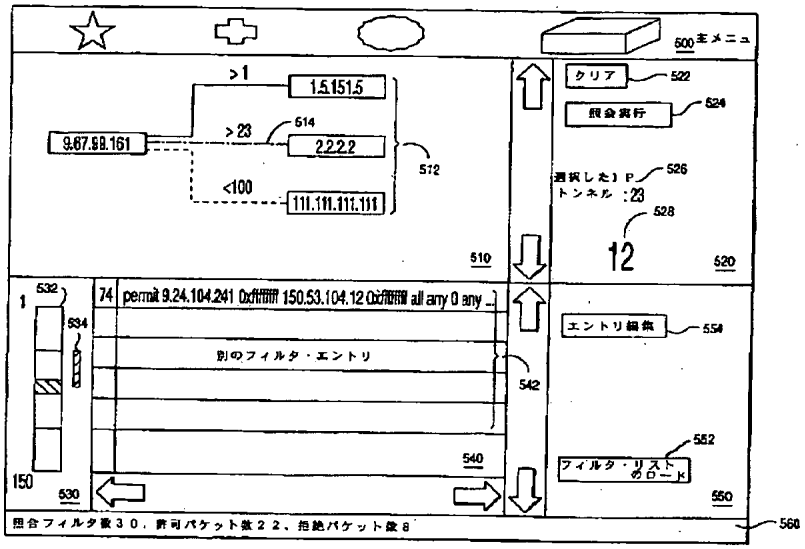
【図５】


900 主メニュー
>1
318
1.5.151.5
314
>23
9.67.99.161
313
317
2222
315
<100
111.111.111.111
316
宛先アドレス
312
310
322
324
326
320
1 96.67.99.161 1.5.151.5 Y Y CDMF 1000 60 1 ACTIVE
23
《別のＩＰトンネル・エントリ》
342
340
符号化および許可
符号化および許可なし
符号化なし、および許可
符号化なし、および許可なし
333
330
エントリ削除
エントリ編集
エントリ活性化
エントリ不活性化
352
ファイアウォールからロード
ファイアウォールへ保存
350
360

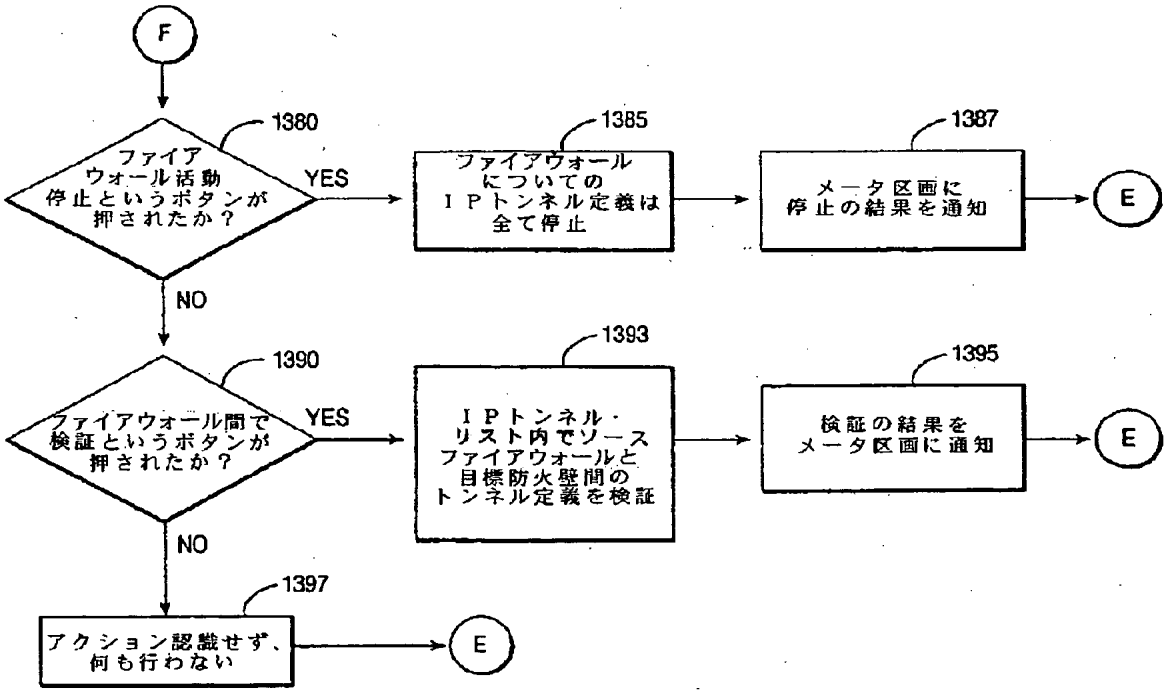
【図６】


400 主メニュー
トンネルＩＤ
ソース・アドレス
宛先アドレス
1.5.151.5
符号化アルゴリズム
別のエントリ・フィールド
《別の照会テストを保存および検索可能》
符号化ポリシィ
410
クリア
422
照会実行
424
423
2
420
1 96.67.99.161 1.5.151.5 Y Y CDMF 1000 60 1 ACTIVE
23
《別のＩＰトンネル・エントリ》
442
440
エントリ編集
454
エントリ削除
トンネル・リスト・リロード
452
450
432
1
434
15
430
照会と照合したＩＰ応答
460

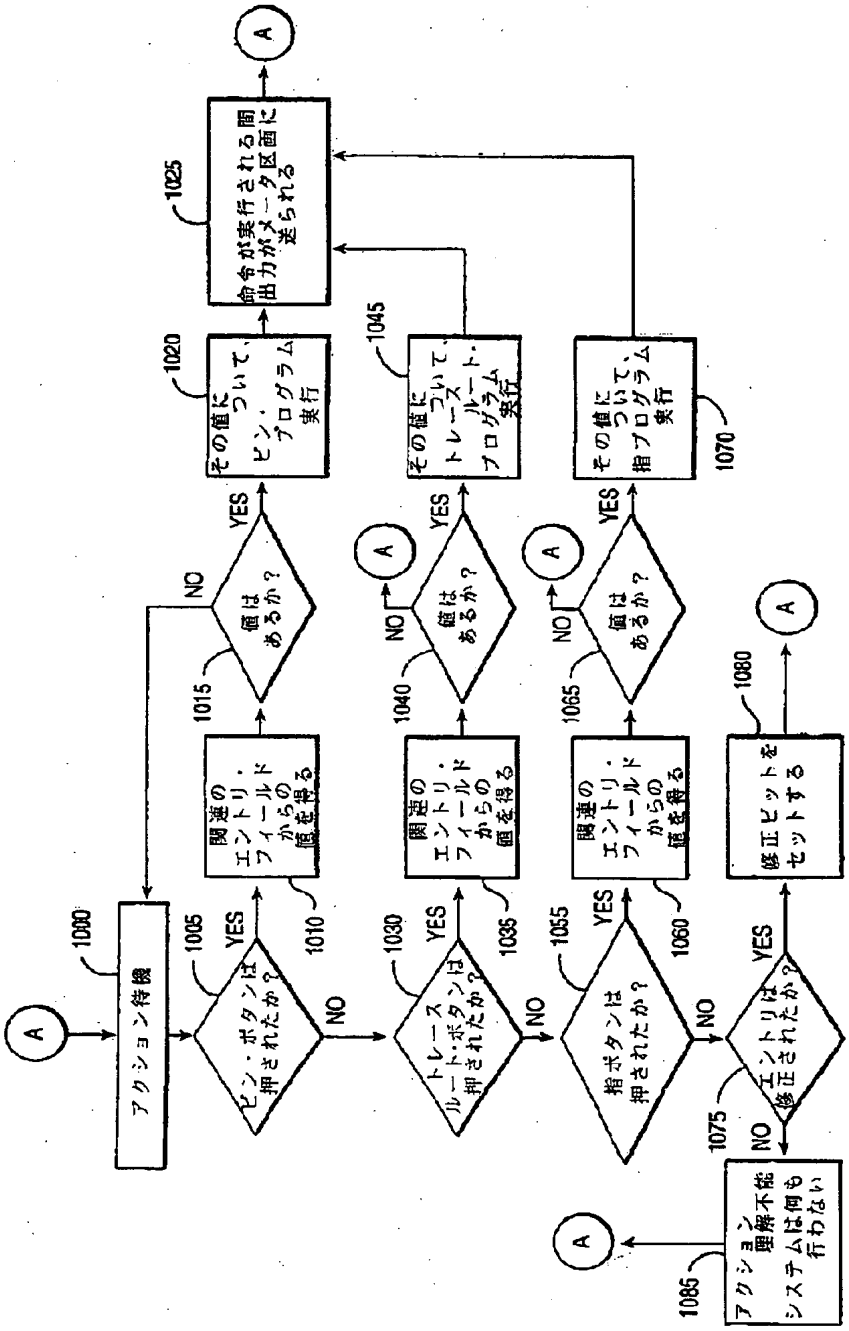
【図７】


600 主メニュ
>1
1.5.151.5
9.67.89.161
>23
514
2.2.2.2
512
<100
111.111.111.111
クリア
522
524
選択したIP
トンネル :23
526
528
12
520
510
532
534
74 permit 9.24.104.241 0xffffffff 150.53.104.12 0xffffffff all any 0 any
別のフィルタ・エントリ
542
エントリ編集
554
552
フィルタ・リスト
のロード
550
540
150
530
照合フィルタ数３０，許可パケット数２２，拒絶パケット数８
560

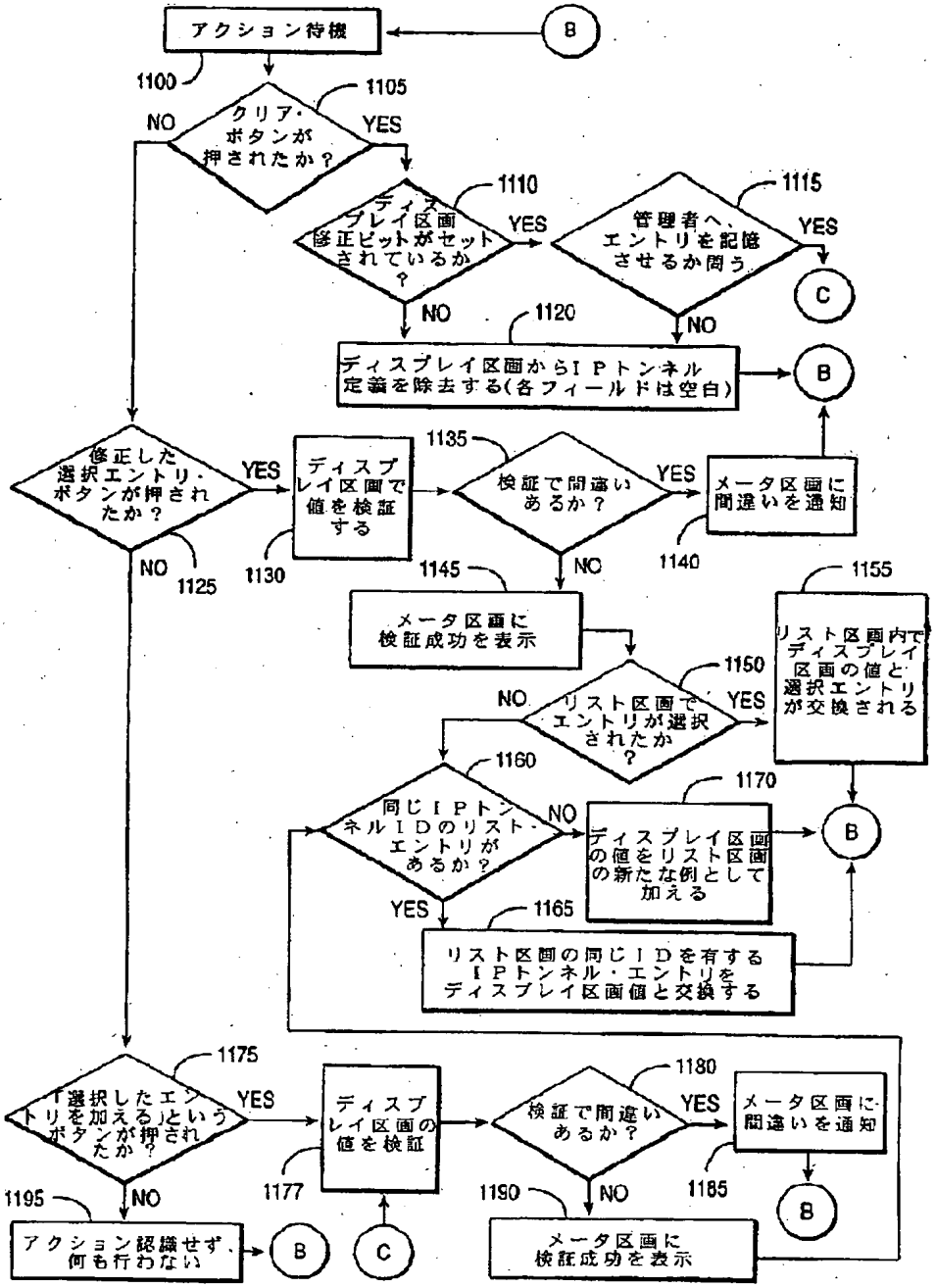
【図１３】


F
1380
ファイア
ウォール活動
停止というボタンが
押されたか？
YES
1385
ファイアウォール
についての
ＩＰトンネル定義は
全て停止
1387
メータ区画に
停止の結果を通知
E
NO
1390
ファイアウォール間で
検証というボタンが
押されたか？
YES
1393
ＩＰトンネル・
リスト内でソース
ファイアウォールと
目標防火壁間の
トンネル定義を検証
1395
検証の結果を
メータ区画に通知
E
NO
1397
アクション認識せず、
何も行わない
E

【図８】


A
1000
アクション待機
1005
ピン・ボタンは押されたか？
YES
NO
1010
関連のエントリ・フィールドからの値を得る
1015
値はあるか？
YES
NO
1020
その値について、ピン・プログラム実行
1025
命令が実行される画出力がメータ区画に送られる
1030
トレース・ルート・ボタンは押されたか？
YES
NO
1035
関連のエントリ・フィールドからの値を得る
1040
値はあるか？
YES
NO
1045
その値について、トレース・ルート・プログラム実行
1055
指ボタンは押されたか？
YES
NO
1060
関連のエントリ・フィールドからの値を得る
1065
値はあるか？
YES
NO
1070
その値について、指プログラム実行
1075
エントリは修正されたか？
YES
NO
1080
修正ヒットをセットする
1085
アクション理解不能システムは何も行わない

【図９】


アクション待機
B
1100
1105
クリア・ボタンが押されたか？
NO
YES
1110
ディスプレイ区画修正ビットがセットされているか？
YES
1115
管理者へ、エントリを記憶させるか問う
YES
C
NO
NO
1120
ディスプレイ区画からＩＰトンネル定義を除去する(各フィールドは空白)
B
修正した選択エントリ・ボタンが押されたか？
YES
ディスプレイ区画で値を検証する
1135
検証で間違いあるか？
YES
メータ区画に間違いを通知
1130
1140
NO
1125
NO
1145
メータ区画に検証成功を表示
1155
リスト区画内でディスプレイ区画の値と選択エントリが交換される
1150
リスト区画でエントリが選択されたか？
NO
YES
1160
同じＩＰトンネルＩＤのリスト・エントリがあるか？
NO
1170
ディスプレイ区画の値をリスト区画の新たな例として加える
B
YES
1165
リスト区画の同じＩＤを有するＩＰトンネル・エントリをディスプレイ区画値と交換する
1175
「選択したエントリを加える」というボタンが押されたか？
YES
ディスプレイ区画の値を検証
1180
検証で間違いあるか？
YES
メータ区画に間違いを通知
1177
1185
B
1195
NO
NO
1190
アクション認識せず、何も行わない
B
C
メータ区画に検証成功を表示